English Translation of Relevant Portions of JP-A-2002-196983
Published on July 12, 2002

:

:

Page (5), column 7, lines 26 -38

[0037] The demodulating means 201 demodulates a received digital broadcast signal. The error correcting means 202 corrects an error in the output of the demodulating means 201. The descrambling means 203 descrambles a signal that has been subjected to error correction. The separating means 204 separates the signal of a selected program from the descrambled signal, and outputs the separated signal. The encrypting means 205 encrypts the separated signal and outputs the encrypted signal. The encryption key generating means 207 generates an encryption key based on the identification data of the encryption key medium means 106, time, and the identification data of the receiver, and feeds the generated encryption key to the encrypting means 205. The authenticating means 206 authenticates the encryption key medium means 106, receives identification data, etc. of the encryption key medium means 106, encrypts the encryption key generated by the encryption key generating means 207, and transfers it to the encryption key medium means 106.

:

:

Page (5), column 7, line 48 –column 8, line 7

[0041] The authenticating means 301 authenticates the encryption key medium means 106, receives an encrypted encryption key, and releases the encryption to obtain the encryption key. The encryption releasing means 302 receives the encrypted signal of a selected program, and releases encryption using the encryption key received from the encryption key medium means 106. The decoding means 303 performs processing such as MPEG decoding on the decrypted signal. The image reproducing means 304 displays an image according to a decoded image signal. The sound reproducing means 305 reproduces sound according to a decoded audio signal, which is outputted via, for example, a speaker.

:

:

Page (6), column 9, line 30 – column 10, line 30

[0056] Fig. 8 is a block diagram showing the configuration of a first embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where an encryption key is mediated by a signal conductor through which the encrypted signal of a program is transmitted. The reference numeral 801 denotes encryption key to heat converting means, and the reference numeral 802 denotes thermal encryption key detecting means.

[0057] The encryption key to heat converting means 801 converts an encryption key generated by the encryption key generating means 207 into a temperature change, changeing the temperature of the signal conductor. The thermal encryption key detecting means 802 detects the temperature change in the signal conductor, converts the temperature change into the encryption key, and feeds it to the encryption releasing means 302.

[0058] With this configuration, the encryption key is transmitted in the form of temperature change, and thus, if the coating of the cable is removed for the purpose of stealing the encryption key, the cable property changes, and thus the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

[0059] Fig. 9 is a block diagram showing the configuration of a second embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where an encryption key is transmitted via a signal conductor through which the encrypted signal of a program is transmitted. The reference numeral 901 denotes encryption key to vibration converting means, and the reference numeral 902 denotes vibration encryption key detecting means.

[0060] The encryption key to vibration-converting means 901 converts the encryption key generated by the encryption key generating means 207 into data that is transmitted in the form of vibration, and this vibrates the signal conductor. The vibration encryption key detecting means 902 detects the data transmitted in the form of vibration, converts it into the encryption key, and

feeds it to the encryption releasing means 302.

[0061] With this configuration, the encryption key is transmitted in the form of vibration, and thus, if the cable is touched for the purpose of stealing the encryption key, the cable property changes, and the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

[0062] Fig. 10 is a block diagram showing the configuration of a third embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where a superconductor is used as a signal conductor. The reference numeral 1001 denotes encryption key to magnetic field converting means, and the reference numeral 1002 denotes resistance encryption key detecting means.

[0063] The encryption key to magnetic field converting means 1001 converts the encryption key generated by the encryption key generating means 207 into a change of magnetic field strength, and applies it to the signal conductor. When the magnetic field is weak, the signal conductor remains superconductive and its resistance is zero. When the magnetic field is strong, the superconductivity of the signal conductor is destroyed and resistance appears therein. The resistance encryption key detecting means 1002 detects whether or not resistance has appeared, converts the detection result into the encryption key, and feeds it to the encryption releasing means 302.

[0064] With this configuration, the encryption key is transmitted in the form of resistance, and thus, if the cable is touched for the purpose of stealing the

encryption key, the cable property changes, and thus the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

:

:

Page (7), column 11, line 48 – column 12, line 8

[0074] The authenticating section 1301 performs authentication between the device and the encryption key mediating unit. The volatile optical memory 1302 temporarily and optically stores the encryption key, with which the program has been encrypted, by use of a fluorescent substance or the like, and then automatically deletes it after a predetermined time has passed. The shutter section 1303 opens and closes a mechanical shutter or a liquid crystal shutter and the like when the encryption key is optically inputted or outputted. The light receiving section 1304 receives the optical pattern of the encryption key stored in the volatile optical memory 1302. The light emitting section 1305 emits light representing the encryption key in the form of an optical pattern. The encryption key converting section 1306 performs conversion between the encryption key and the optical pattern.

:

:

Page (8), column 13, line 21 – Page (9), column 15, line 21

[0088] Fig. 18 is a block diagram showing the configuration of another

embodiment of the encryption key mediating unit of the present invention. The reference numeral 1801 denotes an IC card, the reference numeral 1802 denotes IC card authenticating means, the reference numeral 1803 denotes encrypting/decrypting means, the reference numeral 1804 denotes device authenticating means, and the reference numeral 1805 denotes electromagnetic wave transmitting/receiving means.

[0089] The IC card 1801 stores an encryption key with which a program has been encrypted. The IC card authenticating means 1802 authenticates the IC card 1801, transfers the identification data of the IC card to the apparatus, and transfers an encryption key to the IC card. The encrypting/decrypting means 1803 decrypts an encrypted encryption key received from the apparatus, and then encrypts the decrypted encryption key to be in the state in which the encryption key is stored in the IC card 1801. The device authenticating means 1804 authenticates devices on a transmitting side and on a receiving side, and transmits and receives the encryption key. The electromagnetic wave transmitting/receiving means 1805, for example, uses an infrared ray to communicate with a receiver, and a radio wave to communicate with a presentation device. The electromagnetic wave transmitting/receiving means 1805 can operated such that, when the first and the second digital media devices are located in the vicinity, it uses an infrared ray to communicate with the two apparatuses, and when they are located far away, it uses an infrared ray to communicate with one of them and a radio wave to communicate with the other, or it uses a radio wave to communicate with both of them.

[0090] Thus, with this configuration, an IC card is installed, for example, in a

remote control unit, and thus the IC card can be moved from one device to the other in the remote control unit held in hand. Furthermore, a plurality of IC cards can be inserted into a single remote control unit to operate and authenticate each corresponding device, and thus copy right can be protected without forcing the user to perform an extra operation.

[0091] Fig. 19 is a block diagram showing the configuration of still another embodiment of the encryption key mediating unit. This configuration is obtained by adding device registering means 1901 to the configuration shown in Fig. 18.

[0092] The device registering means 1901 is for registering in advance a device to be used. The device authenticating means 1804 authenticates only a device that is registered in the device registering means 1901.

[0093] Thus, only a registered device is allowed to be used, and this prevents an unacceptable unauthorized device from being used; as a result, copy right can be protected.

[0094] Fig. 20 is a block diagram showing the configuration of still another embodiment of the encryption key mediating unit. The reference numeral 2001 denotes an encryption IC card, the reference numeral 2002 denotes encryption key decrypting means.

[0095] The encryption IC card 2001 encrypts an encryption key, with which a program has been encrypted, with an encryption key corresponding to the second digital media device, and stores the resulting encrypted encryption key. The IC card authenticating means 1802 authenticates the encryption IC card 2001, transfers the identification data of the encryption IC card to the device,

and transfers the encryption key to the IC card. The encryption key decrypting means 2002 decrypts the encrypted encryption key received from the device, and transfers it to the encryption IC card 2001 via the IC card authenticating means 1802. The device authenticating means 1804 authenticates the transmitting side and the receiving side devices, and transmits and receives an encryption key. The electromagnetic wave transmitting/receiving means 1805 uses, for example, an infrared ray to communicate with a receiver, and a radio wave to communicate with a presentation device.

[0096] Thus, a configuration can be achieved in which a remote control unit is used as an encryption key mediating unit corresponding to the transmitting side device, and in the remote control unit is installed an IC card that has an encryption function and corresponds to the second digital media device. This enables each of the first and the second digital media devices to transfer an encryption key using its unique code, and thus different device manufacturers can use different codes. This eliminates the need of publishing the encryption algorithm, making it easier to prevent leakage of the encryption key with which a program is encrypted.

[0097] Fig. 21 is a flow chart showing how a device is authenticated and an encryption key is transferred. Fig. 22 shows the process sequence among a receiver which is the first digital media device on the transmitting side, an encryption key mediating unit, and a presentation device which is the second digital media device on the transmitting side in the case where they are normally authenticated. The same numbers are given to processes that

correspond to those in Fig. 21. In Fig. 22, identification data is denoted by "ID" (hereinafter the same).

[0098] At step 2101, a program to be viewed is selected. At step 2102, an encryption key for encrypting the program is generated. At step 2103, authentication is performed between an encryption key mediating unit and the first digital media device on the transmitting side (e.g., a receiver, a reproducing device). At step 2104, the process branches according to whether or not the device is authenticated; when the device is not authenticated, the process is terminated. When the device is authenticated, the process proceeds to step 2105, where the encryption key is transferred to the encryption key mediating unit. At step 2106, the identification data of the encryption key mediating unit that has been transferred to the device on the transmitting side at the authentication is transferred from the first digital media device to the second digital media device on the receiving side (a presentation device, recording device, etc.). At step 2107, authentication is performed between the encryption key mediating unit and the second digital media device on the receiving side. At step 2108, the process branches according to the authentication result, and, when the device is not authenticated, the process is terminated. At step 2109, the encryption key is transferred from the encryption key mediating unit to the second digital media device on the receiving side.

[0099] As described above, the encryption key mediating unit is authenticated using its identification data that has been sent from the first digital media device on the transmitting side directly to the second digital media device on

the receiving side. As a result, even when an encrypted program data and an encryption key that is being transferred between the encryption key mediating unit and the device are drawn out and delivered, for example, via the Internet, the encryption key mediating unit cannot be authenticated at a recipient. This makes it impossible for the second digital media device on the receiving side to receive the encryption key, and thus illegal reproduction and viewing can be prevented.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-196983
(43)Date of publication of application : 12.07.2002

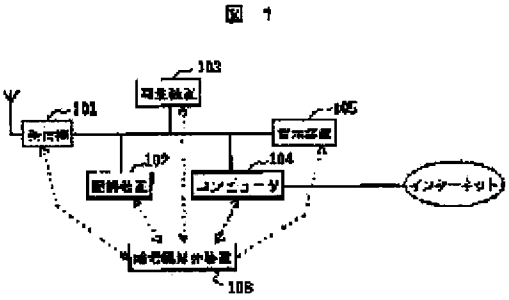
(51)Int.Cl. G06F 12/14
G06K 19/00
H04L 9/08
H04N 5/91
H04N 7/167

(21)Application number : 2000-396576
(22)Date of filing : 27.12.2000

(71)Applicant : HITACHI LTD
(72)Inventor : AKIYAMA MORIYOSHI
SUGIYAMA YOSHIICHI
TAKASHIMIZU SATOSHI
YONEDA SHIGERU
NEMOTO TOSHIYUKI
TSURUGA SADAO
KOREEDA HIROYUKI
OKAMURA TAKUMI

(54) TRANSMITTER FOR ENCODED DIGITAL INFORMATION AND CRYPTOGRAPHY KEY, DIGITAL MEDIA DEVICE, AND CRYPTOGRAPHY KEY MEDIUM DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a new transmitter for encoded digital information and cryptography key, a digital media device, and a cryptography key medium device considering the usability of audiences while protecting copyright.
SOLUTION: This transmitter for the encoded digital information and the cryptography key is provided with first digital media devices 101 and 103, the cryptography key medium device 106, and second digital media devices 105, 102, and 104. The first digital media devices encode the digital information by the cryptography key, output it to the second digital media devices as the encoded digital information, convert the cryptography key into a further encoded public key and output it to the cryptography key medium device. The second digital media devices decode the cryptography key from the public key inputted from the cryptography key medium device and decode the encoded digital information inputted from the first digital media devices by the cryptography key.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－196983
（P2002－196983A）
(43)公開日　平成14年７月12日(2002.7.12)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｋ　19/00		Ｇ０６Ｋ　19/00	Ｑ	５Ｂ０３５
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ	５Ｃ０５３
Ｈ０４Ｎ　5/91			６０１Ｅ	５Ｃ０６４
7/167		Ｈ０４Ｎ　5/91	Ｐ	５Ｊ１０４

審査請求　未請求　請求項の数14　ＯＬ　（全 37 頁）　最終頁に続く

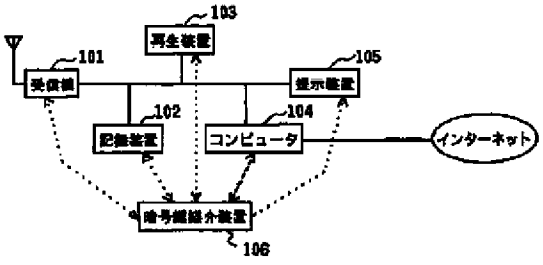
(21)出願番号　特願2000－396576(P2000－396576)
(22)出願日　平成12年12月27日(2000.12.27)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　秋山　守慶
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　杉山　由一
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100068504
弁理士　小川　勝男　（外２名）
最終頁に続く

(54)【発明の名称】　暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置

(57)【要約】
【課題】著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供する。
【解決手段】第１のデジタルメディア機器（１０１，１０３）と暗号鍵媒体装置（１０６）と第２のデジタルメディア機器（１０５，１０２，１０４）を備え、第１のデジタルメディア機器はデジタル情報を暗号鍵で暗号化して暗号化デジタル情報として第２のデジタルメディア機器に出力するとともに、暗号鍵をさらに暗号化した公開鍵にして暗号鍵媒体装置に出力し、第２のデジタルメディア機器は暗号鍵媒体装置から入力された公開鍵より暗号鍵を復号し、暗号鍵により第１のデジタルメディア機器から入力された暗号化デジタル情報を復号する。

図　1



1

【特許請求の範囲】

【請求項１】第１のデジタルメディア機器と、暗号鍵媒体装置と、第２のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、

前記第１のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として前記第２のデジタルメディア機器に出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記暗号鍵媒体装置に出力するように構成し、

前記暗号鍵媒体装置は、前記第１のデジタルメディア機器から入力された前記公開鍵より前記暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして前記第２のデジタルメディア機器に出力するように構成し、

前記第２のデジタルメディア機器は、前記暗号鍵媒体装置から入力された前記公開鍵より前記暗号鍵を復号し、前記暗号鍵により、前記第１のデジタルメディア機器から入力された前記暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置。

【請求項２】デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記出力とは別に出力するように構成したことを特徴とするデジタルメディア機器。

【請求項３】入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項４】入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器。

【請求項５】請求項１記載の前記第１のデジタルメディア機器または請求項２記載の前記デジタルメディア機器がデジタル放送を受信する受信機であって、デジタル放送信号を復調し、誤りを訂正し、スクランブルを解除し、視聴を希望するデジタル情報を選択して分離し、選択されたデジタル情報を、前記暗号鍵で暗号化して出力するように構成したことを特徴とする受信機。

【請求項６】請求項１記載の前記第１のデジタルメディア機器または請求項２記載の前記デジタルメディア機器が再生装置であって、記録媒体からデジタル情報を再生し、前記暗号鍵で暗号化して出力するように構成したことを特徴とすることを特徴とする再生装置。

【請求項７】請求項１記載の前記第１のデジタルメディア機器または請求項４記載の前記デジタルメディア機器が提示装置であって、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号して表示するように構成したことを特徴とする提示装置。

2

【請求項８】請求項１記載の前記第１のデジタルメディア機器または請求項４記載の前記デジタルメディア機器が記録装置であって、入力された公開鍵より公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵をさらに暗号化した公開鍵にして、別に入力された暗号化デジタル情報とともに記録媒体に記録するように構成したことを特徴とする記録装置。

【請求項９】請求項１記載の前記第１のデジタルメディア機器または請求項４記載の前記デジタルメディア機器がコンピュータであって、入力された暗号化デジタル情報を記憶し、別に入力された暗号鍵は記憶しないか入力されないように構成したことを特徴とするコンピュータ。

【請求項１０】請求項１または３記載の前記暗号鍵媒体装置は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶手段に記憶するとともに、前記記憶手段に記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項１１】第１のデジタルメディア機器と、暗号鍵媒体装置と、第２のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、

前記第１のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として前記第２のデジタルメディア機器に出力し、前記暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成し、

前記暗号鍵媒体装置は、前記第１のデジタルメディア機器との認証時に前記暗号鍵媒体装置の識別情報を前記第１のデジタルメディア機器に転送し、前記第１のデジタルメディア機器から前記暗号鍵を入力するように構成し、

前記第２のデジタルメディア機器は、前記暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された前記暗号鍵により、前記第１のデジタルメディア機器から入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置。

【請求項１２】デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成したことを特徴とするデジタルメディア機器。

【請求項１３】第１のデジタルメディア機器との認証時に識別情報を前記第１のデジタルメディア機器に転送し、前記第１のデジタルメディア機器から前記暗号鍵を入力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項１４】暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された暗号鍵により、別に入力さ

れた、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル放送等の送信側デジタルメディア機器から、ＤＶＤレコーダ、Ｄ－ＶＨＳ　ＶＴＲなどの受信側デジタルメディア機器に、暗号化デジタル情報を伝送する際の暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置に関する。

【０００２】

【従来の技術】放送や、パッケージメディアがデジタル化され、劣化することなしに複製を作ることが簡単にできるようになっている。このため、著作権保護のための機能が新たに必要とされるようになった。

【０００３】特に課題となるのがパーソナルコンピュータである。記録できないようなストリーミングコンテンツについても、ディスプレイへのデジタル出力を違法に記録するなどの方法が考えられる。

【０００４】それを防ぐ規格として、HDCP(High-bandwidth Digital Content Protection：White Paper ->http://www.siimage.com/documents/SiI-WP-002-A.pdf)などが、提案されている。

【０００５】これは、パソコンのディスプレイ出力を暗号化し、ディスプレイで復号するというもので、データとは別の線で、鍵交換を行い、認証された場合にのみ暗号化したデータを出力して、表示するというものであった。

【０００６】

【発明が解決しようとする課題】しかしながら、パーソナルコンピュータ以外のＡＶ機器もデジタル化され、さらにそれらが相互に接続されたネットワークを構成するようになると、パソコンとディスプレイという限られた組み合わせ以外での著作権保護が必要となる。

【０００７】また、コンピュータネットワークと、ＡＶ機器のネットワークでは、規格が異なっていたが、ＩＰ over　１３９４など、ＡＶ系のネットワークにコンピュータネットワークと共通のプロトコルを乗せる方法も開発されており、すべてのネットワークを１本の線で接続することも可能となってくる。

【０００８】さらに、コンテンツ提供者の立場からは、コンテンツをインターネットなどに勝手に配信されることに対する不安から、著作権の保護方法が確立しないと、デジタル系のメディアに供給しにくいという課題もある。

【０００９】本発明の目的は、著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供することにある。

【００１０】

【課題を解決するための手段】本発明は、第１のデジタルメディア機器と、暗号鍵媒体装置と、第２のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、前記第１のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記暗号鍵媒体装置に出力するように構成し、前記暗号鍵媒体装置は、前記第１のデジタルメディア機器から入力された前記公開鍵より前記暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして前記第２のデジタルメディア機器に出力するように構成し、前記第２のデジタルメディア機器は、前記暗号鍵媒体装置から入力された前記公開鍵より前記暗号鍵を復号し、前記暗号鍵により、前記第１のデジタルメディア機器から入力された前記暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置である。

【００１１】本発明は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記出力とは別に出力するように構成したことを特徴とするデジタルメディア機器である。

【００１２】本発明は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置である。

【００１３】本発明は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器である。

【００１４】本発明で、前記第１のデジタルメディア機器または前記デジタルメディア機器がデジタル放送を受信する受信機であって、デジタル放送信号を復調し、誤りを訂正し、スクランブルを解除し、視聴を希望するデジタル情報を選択して分離し、選択されたデジタル情報を、前記暗号鍵で暗号化して出力するように構成したことを特徴とする受信機である。

【００１５】本発明で、前記第１のデジタルメディア機器または前記デジタルメディア機器が再生装置であって、記録媒体からデジタル情報を再生し、前記暗号鍵で暗号化して出力するように構成したことを特徴とすることを特徴とする再生装置である。

【００１６】本発明で、前記第１のデジタルメディア機器または前記デジタルメディア機器が提示装置であって、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号して表示するように構成

したことを特徴とする提示装置である。

【００１７】本発明で、前記第１のデジタルメディア機器または請求項４記載の前記デジタルメディア機器が記録装置であって、入力された公開鍵より公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵をさらに暗号化した公開鍵にして、別に入力された暗号化デジタル情報とともに記録媒体に記録するように構成したことを特徴とする記録装置である。

【００１８】本発明で、前記第１のデジタルメディア機器または前記デジタルメディア機器がコンピュータであって、入力された暗号化デジタル情報を記憶し、別に入力された暗号鍵は記憶しないか入力されないように構成したことを特徴とするコンピュータである。

【００１９】本発明で、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶手段に記憶するとともに、前記記憶手段に記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置である。

【００２０】本発明は、第１のデジタルメディア機器と、暗号鍵媒体装置と、第２のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、前記第１のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として前記第２のデジタルメディア機器に出力し、前記暗号鍵媒体装置を認証してから、生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成し、前記暗号鍵媒体装置は、前記第１のデジタルメディア機器との認証時に前記暗号鍵媒体装置の識別情報を前記第１のデジタルメディア機器に転送し、前記第１のデジタルメディア機器から前記暗号鍵を入力するように構成し、前記第２のデジタルメディア機器は、前記暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された前記暗号鍵により、前記第１のデジタルメディア機器から入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置である。

【００２１】本発明は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成したことを特徴とするデジタルメディア機器である。

【００２２】本発明は、第１のデジタルメディア機器との認証時に識別情報を前記第１のデジタルメディア機器に転送し、前記第１のデジタルメディア機器から前記暗号鍵を入力するように構成したことを特徴とする暗号鍵媒体装置である。

【００２３】本発明は、暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された暗号鍵により、別に入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器である。

【００２４】

【発明の実施の形態】図１は、本発明の実施の形態の構成のブロック図を示す。１０１は受信機、１０２はＤ－ＶＨＳ　ＶＴＲやＤＶＤレコーダなどの記録装置、１０３はＤＶＤプレーヤなどの再生装置、１０４はパーソナルコンピュータ（以下ＰＣと略す）などのコンピュータ、１０５はディスプレイ、スピーカなどの提示装置、１０６は暗号鍵を媒介するためのケーブルやＩＣカードその他の機器などの暗号鍵媒介装置である。

【００２５】受信機１０１は、デジタル放送を受信しＭＰＥＧなどのフォーマットの信号に復号し、暗号化を施して出力する。記録装置１０２は、受信機１０１の出力する暗号化された信号を暗号化された状態でパッケージメディアに記録する。この時、暗号化に使用した暗号鍵は、暗号鍵媒介装置１０６を介して暗号化された状態で受け渡され、暗号化された状態で暗号鍵をパッケージメディアに記録する。また、記録装置１０２は、記録した暗号化された状態の信号をそのまま出力すると共に、暗号鍵媒介手段１０６を介して、暗号鍵を出力先に渡す。

【００２６】再生装置１０３は、ＤＶＤなどのパッケージメディアを再生する。コンテンツ自体が暗号化されている場合は、それを解除した後に、再生装置１０３が暗号鍵を生成して暗号化を行い出力する。この際に生成した暗号鍵は暗号鍵媒介手段１０６を介して出力される。

【００２７】コンピュータ１０４は、受信機１０１などから出力される信号を一時的に保管して出力する。暗号化された信号を記録して出力するが、暗号鍵は記録しないで、暗号鍵の識別情報のみを暗号鍵媒介手段１０６から受け取り記録する。

【００２８】提示装置１０５は、暗号化された信号を入力し、暗号鍵媒介手段１０６から受け取った暗号鍵で暗号を解除した後、ＭＰＥＧデコードなどの復号処理を行い、映像、音声を再生し提示する。また、提示装置１０５がディスプレイと複数のスピーカなどに分かれていて、暗号鍵媒介装置１０６がＩＣカードなどの場合には、順々に、ＩＣカードを装着し、すべての暗号鍵を転送しておく。

【００２９】上記において、受信機１０１，再生装置１０３が本発明の第１のデジタルメディア機器に相当し、提示装置１０５，記録装置１０２，コンピュータ１０４が本発明の第２のデジタルメディア機器に相当する。

【００３０】したがって、図１は、第１のデジタルメディア機器（受信機１０１、再生装置１０３）と、第２のデジタルメディア機器（提示装置１０５、記録装置１０２、コンピュータ１０４）と、暗号鍵媒体装置１０６の組み合わせから構成されている。

【００３１】図１において、上記第１のデジタルメディア機器は、受信機１０１と再生装置１０３とが図示されているが、どちらか一方であって機器でもよい。また、

上記第２のデジタルメディア機器は、提示装置１０５と記録装置１０２とコンピュータ１０４とが図示されているが、少なくともひとつの機器であってもよい。

【００３２】そして、第１のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力するとともに、暗号鍵をさらに暗号化した公開鍵にして暗号鍵媒体装置１０６に出力する。

【００３３】暗号鍵媒体装置１０６は、第１のデジタルメディア機器から入力された公開鍵より暗号鍵を復号して記憶するとともに、記憶した暗号鍵を暗号化した公開鍵にして第２のデジタルメディア機器に出力する。

【００３４】第２のデジタルメディア機器は、暗号鍵媒体装置１０６から入力された公開鍵より暗号鍵を復号し、暗号鍵により、第１のデジタルメディア機器から入力された暗号化デジタル情報を復号する。

【００３５】したがって、第１のデジタルメディア機器と第２のデジタルメディア機器との機器間では、暗号化されたデジタル信号しか流れないため、違法にコピーしても再生することができず、著作権を保護することができる。

【００３６】図２は、図１の受信機１０１の第１の実施の形態の構成のブロック図を示す。２０１は復調手段、２０２は誤り訂正手段、２０３はデスクランブル手段、２０４は分離手段、２０５は暗号化手段、２０６は認証手段、２０７は暗号鍵生成手段である。

【００３７】復調手段２０１は、受信したデジタル放送信号を復調する。誤り訂正手段２０２は、復調手段２０１の出力の誤りを訂正する。デスクランブル手段２０３は、誤り訂正した後の信号にデスクランブル処理を行う。分離手段２０４は、デスクランブル済みの信号から選択した番組の信号を分離して出力する。暗号化手段２０５は、分離した信号に暗号化を施して出力する。暗号鍵生成手段２０７は、暗号鍵媒介手段１０６の識別情報や時刻、受信機の識別情報などを元にした暗号鍵を生成し、暗号化手段２０５へ出力する。認証手段２０６は、暗号鍵媒介装置１０６を認証し、識別情報などを受け取り、暗号鍵生成手段２０７の生成した暗号鍵を暗号化して暗号鍵媒介装置１０６へ転送する。

【００３８】以上により、受信機で独自に暗号化を行って選択した番組の信号を出力し、暗号鍵は別系統で出力するために、違法コピーして再生することが困難である。

【００３９】図３は、図１の提示装置１０５の第１の実施の形態の構成のブロック図を示す。

【００４０】３０１は認証手段、３０２は暗号解除手段、３０３は復号手段、３０４は映像再生手段、３０５は音声再生手段である。

【００４１】認証手段３０１は、暗号鍵媒介装置１０６を認証して、暗号化した暗号鍵を受け取り、暗号解除して暗号鍵を取り出す。暗号解除手段３０２は、選択した番組の暗号化された信号を入力し暗号鍵媒介装置１０６から受け取った暗号鍵を用いて暗号を解除する。復号手段３０３は、暗号を解除された信号にＭＰＥＧデコードなどの処理を行う。映像再生手段３０４は、デコードされた映像信号をディスプレイ上に表示する。音声再生手段３０５は、デコードされた音声信号をスピーカなどで再生する。

【００４２】以上により、正規に出力された信号のみ再生することができる。違法にコピーされた信号は再生することができなくなる。

【００４３】図４は、図１の記録装置１０２の第１の実施の形態の構成のブロック図を示す。４０１は認証手段、４０２は暗号鍵用暗号鍵生成手段、４０３は暗号鍵暗号化復号化手段、４０４は記録手段である。

【００４４】認証手段４０１は、暗号鍵媒介装置１０６を認証して、暗号化した暗号鍵を受け取り、暗号解除して暗号鍵を取り出して出力する。また、記録した番組を再生する場合には、暗号鍵を暗号化して暗号鍵媒介装置１０６へ転送する。暗号鍵用暗号鍵生成手段４０２は、認証手段４０１から暗号鍵媒介装置１０６の識別情報を受け取り、暗号鍵を暗号化するための暗号鍵を生成する。暗号鍵暗号化復号化手段４０３は、暗号鍵媒介装置１０６から受け取った暗号鍵に、暗号鍵用暗号鍵生成手段が生成した鍵で暗号化を行う。あるいは、暗号化された暗号鍵の暗号を解除して認証手段へ出力する。記録手段４０４は、選択した番組の暗号化された信号を記録するとともに、暗号鍵暗号化復号化手段４０３で暗号化された暗号鍵を記録する。

【００４５】以上により、違法にコピーしたとしても、暗号鍵をさらに暗号化して記録しているために、再生することができない。

【００４６】図５は、図１の再生装置１０３の第１の実施の形態の構成のブロック図を示す。５０１は認証手段、５０２は暗号鍵生成手段、５０３は暗号化手段、５０４は記録媒体である。

【００４７】認証手段５０１は、暗号鍵媒介装置１０６を認証し、暗号鍵生成手段５０２の生成した暗号鍵を暗号化して暗号鍵媒介装置１０６へ転送する。暗号鍵生成手段５０２は、認証手段５０１から受け取った暗号鍵媒介装置１０６の識別情報などを元に暗号鍵を生成する。暗号化手段５０３は、記憶媒体５０４から出力するコンテンツの信号に暗号鍵生成手段５０２で生成した暗号鍵で、暗号化を施して出力する。記憶媒体５０４は、市販のＤＶＤやＤ－ＶＨＳなどのパッケージメディアである。

【００４８】以上により、パッケージメディアの再生時に、独自の暗号化を施して出力するため、違法コピーを防ぐことができる。

【００４９】図６は、図１のコンピュータ１０３の第１の実施の形態の構成のブロック図を示す。

【００５０】６０１は認証手段、６０２は演算手段、６０３は記憶装置、６０４は映像音声変換装置である。

【００５１】認証手段６０１は、暗号鍵媒介装置１０６を認証し、暗号鍵の識別情報を受け取る。演算装置６０２は、認証手段から出力される暗号鍵の識別情報と、外部から入力した暗号化された番組の信号を入力し、記憶装置６０３へ記憶する。また、記憶装置６０３に記憶している番組の信号を外部へ出力すると同時に、暗号鍵の識別情報を認証手段６０１へ出力する。映像音声変換装置６０４は、コンピューター内部で生成した映像、音声データを提示装置１０５で提示したり、記録手段１０２で記録する形式の信号に変換して出力する。

【００５２】以上により、コンピュータ内部には、暗号化された信号のみを入力し、暗号鍵は入力されないため、インターネットなどに違法に配信しても、暗号鍵がないため再生できず、著作権を保護することができる。

【００５３】図７は、図１の提示装置１０５の第２の実施の形態の構成のブロック図を示す。本構成では、図３の第１の実施の形態の構成に、入力先機器判定手段７０１と入力手段７０２が加えられている。

【００５４】入力手段７０２は、各構成機器の操作を入力する。入力先機器判定手段７０１は、入力手段７０２から入力した操作がどの機器に対するものかを判定して、その操作を対象となる機器へ転送する。

【００５５】以上により、本構成例は、操作を提示手段に対してのみ行えばよいため、他の機器は、見えない場所に隠れていてもよい。このため、所有者以外の人間が機器を分解して内部の信号を盗むといったことを防ぐことも可能である。

【００５６】図８は、暗号鍵媒介装置の第１の実施の形態の構成のブロック図を示す。この図では、受信機１０１と提示装置１０５を接続する場合の例で、暗号鍵の媒介に暗号化した番組を伝送する信号線を使用する場合を示している。８０１は暗号鍵熱変換手段、８０２は熱暗号鍵検出手段である。

【００５７】暗号鍵熱変換手段８０１は、暗号鍵生成手段２０７で生成した暗号鍵を温度変化に変換して、信号線の温度を変化させる。熱暗号鍵検出手段８０２は、信号線の温度変化を検出し、暗号鍵へ変換して、暗号鍵解除手段３０２へ出力する。

【００５８】本構成では、暗号鍵を温度変化として伝送するため、暗号鍵を盗もうとしてケーブルの被服を破ったりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【００５９】図９は、暗号鍵媒介装置の第２の実施の形態の構成のブロック図を示す。この図では、受信機１０１と提示装置１０５を接続する場合の例で、暗号鍵の媒介に暗号化した番組を伝送する信号線を使用する場合を示している。９０１は暗号鍵振動変換手段、９０２は振動暗号鍵検出手段である。

【００６０】暗号鍵振動変換手段９０１は、暗号鍵生成手段２０７で生成した暗号鍵を振動による伝達情報に変換して、信号線を振動させる。振動暗号鍵検出手段９０２は、信号線の振動による伝達情報を検出し、暗号鍵へ変換して、暗号鍵解除手段３０２へ出力する。

【００６１】本構成では、暗号鍵を振動として伝送するため、暗号鍵を盗もうとしてケーブルに接触したりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【００６２】図１０は、暗号鍵媒介装置の第３の実施の形態の構成のブロック図を示す。この図では、受信機１０１と提示装置１０５を接続する場合の例で、超伝導体を用いた信号線を使用する場合を示している。１００１は暗号鍵磁界変換手段、１００２は抵抗暗号鍵検出手段である。

【００６３】暗号鍵磁界変換手段１００１は、暗号鍵生成手段２０７で生成した暗号鍵を磁界の強度変化に変換して、信号線に加える。磁界が弱い場合は、信号線は超伝導状態を維持し電気抵抗が０になる。磁界が強い場合には、超伝導を破壊して電気抵抗が表れる。抵抗暗号鍵検出手段１００２は、信号線の抵抗のあるなしを検出し、暗号鍵へ変換して、暗号鍵解除手段３０２へ出力する。

【００６４】本構成では、暗号鍵を抵抗として伝送するため、暗号鍵を盗もうとしてケーブルに接触したりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【００６５】図１１は、暗号鍵媒介装置の第４の実施の形態の構成のブロック図を示す。１１０１は暗号鍵生成手段、１１０２は認証手段、１１０３は乱数発生手段、１１０４は記憶手段、１１０５は暗号化復号化手段である。

【００６６】第１のデジタルメディア機器（受信機、再生装置など）に接続する場合、暗号鍵生成手段１１０１は、認証用の共通鍵と、番組を暗号化した暗号鍵を転送する際に使用する公開鍵とそれを復号する秘密鍵を生成する。乱数発生手段１１０３は、認証に使用する第２の乱数値を生成する。認証手段１１０２は、送信側機器から第１の乱数値を受け取り暗号鍵生成手段１１０１に第１の共通鍵を生成させ、暗号化復号化手段１１０５に第１の共通鍵で第２の乱数値を暗号化させて、暗号化した第２の乱数値を認証情報として、第２の乱数値とともに送信側機器に転送する。

【００６７】第２の乱数値を元に生成した第２の共通鍵で、暗号鍵媒介手段１０６自身の識別情報を暗号化したものを送信側機器に転送する。暗号化復号化手段１１０５は、暗号鍵生成手段１１０１で生成した第１の共通鍵

で乱数発生手段１１０３が発生した乱数を暗号化し、第２の共通鍵で、暗号鍵媒介手段１０６の識別情報を暗号化する。また、暗号鍵生成手段１１０１で生成した公開鍵で暗号化された送信側機器から送られた暗号鍵を暗号鍵生成手段１１０１で生成した秘密鍵で復号する。記憶手段１１０４は、暗号化復号化手段１１０５で復号された暗号鍵を記憶する。

【００６８】第２のデジタルメディア機器（提示装置、記録装置など）に接続する場合、暗号鍵生成手段１１０１は、受信側機器から転送された第３の乱数値を元に第３の共通鍵を生成する。暗号化復号化手段１１０５は、第３の共通鍵で暗号鍵媒介手段１０６の識別情報を暗号化して受信側機器へ転送する。また、受信側機器から転送された公開鍵で、記憶手段１１０４に記憶している暗号鍵を暗号化して出力する。認証手段１１０２は、受信側機器から第３の乱数値、公開鍵を受け取り、第３の共通鍵で暗号化した識別情報と、公開鍵で暗号化した暗号鍵を受信側機器へ転送する。

【００６９】第２のデジタルメディア機器は、第１のデジタルメディア機器から転送された暗号鍵媒介手段の識別情報と、暗号鍵媒介手段から直接転送された識別情報が一致するかで認証を行うことにより、暗号鍵媒介装置から暗号鍵が盗まれても、暗号化した番組を再生できないようにすることができる。

【００７０】図１２は、図１１の認証手段１１０２の構成のブロック図を示す。１２０１は提示手段、１２０２は認識手段、１２０３は変換手段、１２０４は処理部である。

【００７１】提示手段１２０１は、暗号化した暗号鍵、公開鍵及び乱数値を２次元の光学パターンとして提示する。認識手段１２０２は、２次元の光学パターンを認識する。変換手段１２０３は、電気的な信号と光学パターンのデータとを変換する。処理部１２０４は、変換手段１２０３から出力される信号を入力し、認証処理を行う。暗号鍵媒介手段においては、暗号鍵生成手段１１０１、乱数発生手段１１０３、暗号化復号化手段１１０５に対して暗号鍵データや乱数値データを振り分けて処理を行わせる。

【００７２】以上により、光学的に暗号鍵の受け渡しを行うため、短時間に大量の暗号鍵データを転送でき、待ち時間なしに操作を行うことができる。

【００７３】図１３は、暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の認証手段の第１の実施の形態の構成のブロック図を示す。１３０１は認証部、１３０２は揮発性光学メモリ、１３０３はシャッター部、１３０４は受光部、１３０５は発光部、１３０６は暗号鍵変換部である。

【００７４】認証部１３０１は、機器と暗号鍵媒介装置の間で認証処理を行う。揮発性光学メモリ１３０２は、番組を暗号化した暗号鍵を蛍光物質などで光学的に一時的に記憶し、一定時間経過後には自動的に消去する。シャッター部１３０３は、暗号鍵を光学的に入力あるいは出力する際に機械的あるいは液晶などのシャッターを開閉する。受光部１３０４は、揮発性光学メモリ１３０２に記憶している暗号鍵の光学的パターンを受光する。発光部１３０５は、暗号鍵を光学的なパターンとして発光する。暗号鍵変換部１３０６は、暗号鍵と光学的パターンとの変換処理を行う。

【００７５】以上により、暗号鍵媒介装置のシャッター部を強制的に開放すると光を受けて、暗号鍵が消去される、また、長時間放置していても揮発して消去されるために、暗号鍵を盗むことが困難になり、著作権を保護することができる。

【００７６】図１４は、暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の認証手段の第２の実施の形態の構成のブロック図を示す。１４０１は記録部、１４０２は温度感応発生部、１４０３は暗号鍵変換部である。

【００７７】認証部１３０１で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部１４０１に暗号鍵を記録する。温度感応発生部は、暗号鍵を温度変化に変換して、機器の認証手段と暗号鍵媒介装置１０６の間で受け渡しを行う。暗号鍵変換部１４０３は、温度変化から暗号鍵へ変換する。

【００７８】以上により、本構成では、暗号鍵を温度変化として受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【００７９】図１５は、暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の第３の実施の形態の構成のブロック図を示す。１５０１は圧力感応発生部、１５０２は暗号鍵変換部である。

【００８０】認証部１３０１で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部１４０１に暗号鍵を記録する。圧力感応発生部１５０１は、暗号鍵を圧力変化に変換して、機器の認証手段と暗号鍵媒介装置１０６の間で受け渡しを行う。暗号鍵変換部１５０２は、圧力変化から暗号鍵へ変換する。

【００８１】以上により、本構成では、暗号鍵を圧力変化として受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【００８２】図１６は、暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の認証手段の第４実施の形態の構成のブロック図を示す。１６０１は超音波発生受信部部、１６０２は暗号鍵変換部である。

【００８３】認証部１３０１で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部１４０１に暗号鍵を記録する。超音波発生受信部１６０１は、暗号鍵を超音波信号に変換して、機器の認証手段と暗号鍵媒介装置１０６の間で受け渡しを行う。

暗号鍵変換部１６０２は、超音波信号から暗号鍵へ変換する。

【００８４】以上により、本構成では、暗号鍵を超音波で受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【００８５】図１７は、暗号鍵媒介装置の他の構成を示す図である。１７０１は可動導体、１７０２は接点である。

【００８６】可動導体１７０１が第１のデジタルメディア機器にあり、第２のデジタルメディア機器の接点１７０２に接続することができる。暗号鍵は複数の可動導体１７０１を第２のデジタルメディア機器の接点１７０２に接続する、しないの組み合わせパターンと、可動導体１７０１の内部を伝送する信号の組み合わせによって伝達する。また、単純に可動導体を接続する接続しないという状態を用いるだけではなく、可動導体の先端部を複数の位置に移動するようにして、より複雑なパターンを伝送することも可能である。

【００８７】以上により、暗号鍵の盗用が困難になり、著作権の保護ができる。

【００８８】図１８は、暗号鍵媒介装置の別の実施の形態の構成のブロック図を示す。１８０１はＩＣカード、１８０２はＩＣカード認証手段、１８０３は暗号化復号化手段、１８０４は機器認証手段、１８０５は電磁波送受信手段である。

【００８９】ＩＣカード１８０１は、番組を暗号化した暗号鍵を記憶する。ＩＣカード認証手段１８０２は、ＩＣカード１８０１を認証し、ＩＣカードの識別情報を機器へ転送するとともに暗号鍵をＩＣカードへ転送する。暗号化復号化手段１８０３は、機器から受け取った暗号化された暗号鍵を復号し、ＩＣカード１８０１に保管する状態での暗号化を施す。機器認証手段１８０４は、送信側、受信側の機器を認証し、暗号鍵の送受信を行う。電磁波送受信手段１８０５は、機器とのやりとりを行う際に、例えば、受信機との間では赤外線を使用し、提示装置に対しては電波で通信するといったことを行う。第１のデジタルメディア機器と第２のデジタルメディア機器が近接した場所にある場合には、どちらも赤外線を使用して通信を行い、離れた場所にある場合には、片方を赤外線、もう一方を電波で通信する、あるいは、両方とも電波で通信を行うといった形態での使用が可能である。

【００９０】以上により、本構成では、リモコンなどにＩＣカードを装着して使用する形態となり、機器間でＩＣカードなどを移動させる場合でも手元で行うことができる。また、複数のＩＣカードを１台のリモコンに挿入して、各機器の操作および認証を行う構成なども可能となり、使用者に余分な操作を強いることなく著作権の保護ができる。

【００９１】図１９は、暗号鍵媒介装置のさらに別の実施の形態の構成のブロック図を示す。図１８の構成に、機器登録手段１９０１を追加した構成である。

【００９２】機器登録手段１９０１は、使用する機器を事前に登録する。機器認証手段１８０４は、機器登録手段１９０１で登録されている機器に対してのみ認証を行う。

【００９３】以上により、事前に登録した機器以外使用できないため、対応していない不正な機器は使用できなくなり、著作権を保護することができる。

【００９４】図２０は、暗号鍵媒介装置のさらに別の実施の形態の構成例のブロック図を示す。２００１は暗号化ＩＣカード、２００２は暗号鍵復号化手段である。

【００９５】暗号化ＩＣカード２００１は、番組を暗号化した暗号鍵を第２のデジタルメディア機器と対応する暗号鍵で暗号化して記憶する。ＩＣカード認証手段１８０２は、暗号化ＩＣカード２００１を認証し、暗号化ＩＣカードの識別情報を機器へ転送するとともに暗号鍵をＩＣカードへ転送する。暗号鍵復号化手段２００２は、機器から受け取った暗号化された暗号鍵を復号し、ＩＣカード認証手段１８０２を介して、暗号化ＩＣカード２００１に転送する。機器認証手段１８０４は、送信側、受信側の機器を認証し、暗号鍵の送受信を行う。電磁波送受信手段１８０５は、機器とのやりとりを行う際に、例えば、受信機との間では赤外線を使用し、提示装置に対しては電波で通信するといったことを行う。

【００９６】以上により、送信側の機器と対になった暗号鍵媒介装置としてリモコンを使用し、第２のデジタルメディア機器と対になった暗号化機能を備えたＩＣカードをリモコンに装着する構成が可能となる。これにより、第１のデジタルメディア機器と第２のデジタルメディア機器それぞれが独自の暗号を使用した暗号鍵の転送を行うことができるため、機器の製造者ごとに異なる暗号を用いることができ、暗号アルゴリズムを公開する必要が無くなる。このため、番組を暗号化した暗号鍵の漏洩を防ぎやすくなる。

【００９７】図２１は、機器を認証して暗号鍵を転送する処理の流れ図を示す。また、図２２は、正常に認証される場合の送信側の第１のデジタルメディア機器である受信機と暗号鍵媒介装置、送信側の第２のデジタルメディア機器である提示装置の間の処理シーケンスを示す。対応する処理に図２１と同じ番号が付されている。ただし、図２２では、識別情報をＩＤと記載してある（以下同様）。

【００９８】ステップ２１０１は、視聴する番組を選択する。ステップ２１０２は、視聴する番組を暗号化する暗号鍵を生成する。ステップ２１０３は、暗号鍵媒介手段と送信側の第１のデジタルメディア機器（受信機、再生装置など）の間で認証を行う。ステップ２１０４は、認証処理の結果、正しい機器かどうかで処理を分岐し、認証されなかった場合には、処理を終了する。ステップ

２１０５は正しい機器だった場合で、暗号鍵媒介装置へ暗号鍵を転送する。ステップ２１０６は、認証時に送信側機器へ転送した暗号鍵媒介装置の識別情報を第１のデジタルメディア機器から受信側の第２のデジタルメディア機器（提示装置、記録装置など）へ転送する。ステップ２１０７は、暗号鍵媒介装置と受信側の第２のデジタルメディア機器の間での認証を行う。ステップ２１０８は、認証の結果が正しいかどうかで処理を分岐し、認証されなかった場合は処理を終了する。ステップ２１０９は、暗号鍵媒介装置から受信側の第２のデジタルメディア機器へ暗号鍵を転送する。

【００９９】以上により、送信側の第１のデジタルメディア機器から直接受信側の第２のデジタルメディア機器に送られた暗号鍵媒介装置の識別情報を使って、暗号鍵媒介装置の認証を行うため、暗号化された番組データと、暗号鍵媒介装置と受け渡し中の暗号鍵を取り出してインターネットなどに配信したりしても、配信先では、暗号鍵媒介装置を認証することができない。このため、受信側の第２のデジタルメディア機器が暗号鍵を受け取ることができず、違法に再生して視聴することを防ぐことができる。

【０１００】図２３は、暗号鍵媒介装置と機器の認証処理だけの流れ図を示す。また、図２４は、受信機と暗号鍵媒介装置、提示装置の間の処理シーケンスを示す。対応する処理に図２２と同じ番号が付されている。

【０１０１】ステップ２３０１は、送信側機器が暗号鍵媒介装置へ時刻などに応じた乱数値を転送する。ステップ２３０２は、送信側機器と暗号鍵媒介装置が乱数値を元に第１の共通鍵を生成する。ステップ２３０３は、暗号鍵媒介装置が第２の乱数値を生成し、第２の乱数値を第１の共通鍵で暗号化したものと共に送信側機器へ転送する。ステップ２３０４は、送信側機器が第２の乱数値と、第１の共通鍵で暗号化した第２の乱数値を復号したものが、同一であることを確認する。ステップ２３０５は、第２の乱数値を元に、送信側機器と暗号鍵媒介装置が第２の共通鍵を生成する。ステップ２３０６は、第２の共通鍵で暗号鍵媒介装置の識別情報を暗号化して、送信側機器へ転送する。ステップ２３０７は、暗号鍵媒介装置の識別情報を第２の共通鍵で復号する。ステップ２３０８は、送信側機器が記録装置の場合には、記録している識別情報と一致するかを確認する。

【０１０２】ステップ２３０９は、受信側機器が公開鍵を送信側機器へ転送する。ステップ２４１０は、送信側機器が、受信側機器の公開鍵で、暗号鍵媒介装置の識別情報を暗号化する。ステップ２４１３は、暗号化した識別情報を受信側機器へ転送する。ステップ２４１４は、受信側機器が対応した秘密鍵を使って、暗号鍵媒介装置の識別情報を復号する。ステップ２４１３は、受信側機器が第３の乱数値を生成し暗号鍵媒介装置へ転送する。

【０１０３】ステップ２４１４は、暗号鍵媒介装置と受信側機器が、第３の乱数値をもとに第３の暗号鍵を生成する。ステップ２４１５は、暗号鍵媒介装置が識別情報を第３の暗号鍵で暗号化して受信側機器へ転送する。ステップ２４１６は、受信側機器が識別情報を復号して、送信側機器から転送されたＩＣカードの識別情報と一致すること確認する。ステップ２４１７は、受信側機器が記録装置の場合に、ＩＣカードの識別情報を記録する。

【０１０４】以上により、送信側機器と受信側機器と、暗号鍵媒介装置の３者の間で認証が成立しない限り視聴することも、記録することもできないため、なんらかの方法で違法コピーしても再生することができず、著作権を保護することができる。

【０１０５】図２５は、暗号鍵を送信側機器から受信側機器へ転送する処理だけの流れ図を示す。図２６は、受信機と暗号鍵媒介装置、提示装置の間の処理シーケンスを示す。対応する処理に図２３と同じ番号がふされている。

【０１０６】ステップ２５０１は、暗号鍵媒介装置が公開鍵を送信側機器へ転送する。ステップ２５０２は、送信側機器が番組を暗号化するのに使用した暗号鍵を、暗号鍵媒介手段の公開鍵で暗号化する。ステップ２５０３は、暗号化した暗号鍵を暗号鍵媒介装置へ転送する。ステップ２５０４は、暗号鍵媒介装置が対応した秘密鍵で暗号鍵を復号する。ステップ２５０５は、受信側機器の公開鍵を暗号鍵媒介装置へ転送する。ステップ２５０６は、暗号鍵媒介装置が、受信側機器の公開鍵で暗号鍵を暗号化する。ステップ２５０７は、暗号化した暗号鍵を受信側機器へ転送する。ステップ２５０８は、受信側機器が対応した秘密鍵で、暗号鍵を復号する。ステップ２５０９は、受信側機器が記録装置の場合には、暗号鍵を独自に暗号化して記録する。

【０１０７】以上により、認証された相手の公開鍵で暗号鍵を暗号化して渡すため、認証されない不正な機器には暗号鍵を転送しないため、著作権を保護できる。

【０１０８】図２７は、暗号鍵媒介装置として、送信側機器と受信側機器を直接接続する形態をとる場合の認証と暗号鍵の転送処理の流れ図を示す。

【０１０９】ステップ２７０１は、送信側機器が公開鍵を受信側機器へ転送する。ステップ２７０２は、受信側機器が乱数を発生し、受信側機器の識別情報と共に、送信側機器の公開鍵で暗号化して、送信側機器へ転送する。ステップ２７０３は、送信側機器が秘密鍵で、受信側機器の識別情報と乱数を復号する。ステップ２７０４は、送信側機器と受信側機器が乱数を元に共通鍵を生成する。この際に、送信側機器は、複数の受信側機器から送られた乱数値の中から、使用する受信側機器(提示装置のみ、提示装置と記録装置、記録装置のみなど)の乱数値を選択して共通鍵を生成する。

【０１１０】ステップ２７０５は、送信側機器が、暗号鍵と送信する受信側機器の識別情報を共通鍵で暗号化し

て、受信側機器へ転送する。ステップ２７０６は、受信側機器が自分あてに送られてきた暗号鍵を、共通鍵で復号する。

【０１１１】以上により、複数の機器が接続された状態で、目的とする機器にのみ暗号鍵を転送することができ、他の機器で番組を再生したり、記録したりすることを防ぐことができる。

【０１１２】図２８は、ＰＣなどのコンピュータへ出力する場合の処理の流れ図を示す。

【０１１３】ステップ２８０１は、出力先にコンピュータを選択する。ステップ２８０２は、記録する番組を選択する。ステップ２８０３では、送信側機器が、選択した番組を暗号化する暗号鍵を生成する(記録装置の場合は、記録している暗号鍵の暗号を解除する)。ステップ２８０４では、暗号鍵媒介装置を認証する。ステップ２８０５では、認証結果が正しいかどうかで処理を分岐し、正しくない場合には終了する。

【０１１４】ステップ２８０６は、正しく認証した場合で、暗号鍵媒介装置へ暗号化した暗号鍵を転送する。ステップ２８０７は、暗号鍵媒介装置からコンピュータへ、暗号鍵の識別情報のみを転送する。ステップ２８０８は、コンピュータが、暗号鍵の識別情報と暗号化された番組を記録する。

【０１１５】以上により、コンピュータに記録する場合は、暗号鍵を記録しないため、インターネットへ配信して、視聴させるといったことを防ぐことができる。

【０１１６】図２９は、ＰＣなどのコンピュータが送信側機器になった場合に視聴する処理の流れ図を示す。

【０１１７】ステップ２９０１は、出力先の機器（提示装置、記録装置など）を選択する。ステップ２９０２は、視聴あるいは記録する番組を選択する。ステップ２９０３は、暗号鍵の識別情報を暗号鍵媒介装置へ転送する。ステップ２９０４は、出力先の機器の認証を行う。ステップ２９０５は、認証結果が正しいかどうかで処理を分岐し、正しくない場合には終了する。ステップ２９０６は、正しく認証された場合で、暗号鍵媒介装置から暗号鍵を出力先機器へ転送する。ステップ２９０７は、コンピュータから暗号化された番組を出力先へ転送する。

【０１１８】以上により、コンピュータ単体では、再生して視聴することができなくて、正規の提示装置と接続して初めて視聴できる。また、正規の記録装置に対してのみ記録させることが可能となり、違法な機器やネットワークに配信して利用させることを防ぐことができる。

【０１１９】図３０，図３１，図３２は、記録に制限がある場合を含めた処理の流れ図を示す。

【０１２０】ステップ３００１は、出力先の機器を選択する。ステップ３００２は、視聴あるいは、記録する番組を選択する。ステップ３００３は、出力先が提示装置かどうかを判定する。ステップ３００４は、出力先が提示装置で無い場合で、記録手段かどうかの判定処理へ分岐する。

【０１２１】ステップ３００５は出力先が提示装置だった場合で、暗号鍵媒介装置の認証を行う。ステップ３００６は、暗号鍵媒介装置へ暗号鍵と、複写属性情報を転送する。ステップ３００７は、暗号鍵媒介装置と提示装置の間で認証を行う。ステップ３００８は、暗号鍵媒介装置から提示装置へ暗号鍵を転送する。

【０１２２】ステップ３００４へ分岐した後は、ステップ３００９で、出力先が記録装置かどうか判定する。ステップ３０１０は、記録装置ではなかった場合で、出力先がコンピュータかどうかの判定処理へ分岐する。

【０１２３】ステップ３０１１は、出力先が記録装置であった場合で、選択した番組が複写を許可されているかどうかを判定し、許可されていない場合には処理を終了する。

【０１２４】ステップ３０１２は、複写が許可されていた場合で、この場合には、複写が１回のみ許可されているかどうかを判定する。ステップ３０１３は、１回のみ複写が許可されている場合で、暗号鍵媒介装置の認証を行う。ステップ３０１４は、暗号鍵媒介装置へ暗号鍵と、１回のみ複写可の複写属性情報を転送する。ステップ３０１５は、暗号鍵媒介装置と記録装置間で認証を行う。ステップ３０１６は、暗号鍵媒介装置から暗号鍵と、複写禁止に変更した複写属性情報を記録装置へ転送する。暗号鍵媒介装置内に保管している複写属性情報も、複写禁止に変更する。ステップ３０１７は、記録装置が暗号鍵を独自に暗号化して記録する。ステップ３０１８は、記録装置に暗号化した番組と複写禁止の複写属性情報を記録する。

【０１２５】ステップ３０１９は、複写回数が１回に制限されていない場合で、暗号鍵媒介装置の認証を行う。ステップ３０２０は、暗号鍵媒介装置へ暗号鍵と複写許可の複写属性情報を転送する。ステップ３０２１は、暗号鍵媒介装置と記録装置の間で認証を行う。ステップ３０２２は、暗号鍵媒介装置から暗号鍵と、複写許可の複写属性情報を記録装置へ転送する。ステップ３０２３は、記録装置が暗号鍵を独自に暗号化して記録する。ステップ３０２４は、記録装置に暗号化した番組と複写許可の複写属性情報を記録する。

【０１２６】ステップ３０１０へ分岐した後は、ステップ３０２５で、出力先がＰＣなどのコンピュータかどうかを判定し、コンピュータでもない場合は、終了する。（他に出力先として使用できる機器がある場合には、さらに分岐して、処理を行う）ステップ３０２６は、出力先がコンピュータの場合で、選択した番組が複写制限なしかどうかを判定し、複写制限がある場合には、終了してコンピュータに対しては、何も出力しない。ステップ３０２７は、複写制限が無い場合で、暗号鍵媒介装置を認証する。ステップ３０２８は、暗号鍵媒介装置へ暗号

鍵と出力先がコンピュータであるという出力先情報を転送する。ステップ３０２９は、暗号鍵媒介装置から暗号鍵の識別情報をコンピュータへ転送する。ステップ３０３０は、コンピュータに暗号化した番組と暗号鍵の識別情報を記録する。

【０１２７】以上により、記録するのに制限がある場合にも対応して処理を行う。コンピュータには、制限のある番組を記録しないことで、違法なコピーを防ぎ、著作権を保護することができる。

【０１２８】図３３は、暗号鍵媒介装置がリモコンなどを兼用して、提示装置と対になったＩＣカードを装着する形態の場合の処理の流れ図を示す。また、図３４は、受信機と暗号鍵媒介装置、ＩＣカード、提示装置の間の処理シーケンスを示す。対応する処理に図３３と同じ番号が付されている。

【０１２９】ステップ３３０１は、提示装置と対になったＩＣカードを暗号鍵媒介装置へ装着する。ステップ３３０２は、暗号鍵媒介装置とＩＣカードが認証処理を行う。ステップ３３０３は、視聴あるいは記録する番組を選択する。ステップ３３０４は、暗号鍵媒介装置が送信側機器を認証する。ステップ３３０５は、暗号鍵を送信側機器と暗号鍵媒介装置の間の専用の暗号化処理を行って、暗号鍵媒介装置へ転送する。

【０１３０】ステップ３３０６は、暗号鍵媒介装置が暗号鍵の暗号を解除する。ステップ３３０７は、解除した暗号鍵をＩＣカードの識別情報を元にした共通鍵で暗号化を施す。ステップ３３０８は、ＩＣカードへ暗号化した暗号鍵を転送する。ステップ３３０９は、暗号鍵媒介装置と受信側機器がＩＣカードの識別情報などを使用して認証処理を行う。ステップ３３１０は、暗号化した暗号鍵を使用するときに、ＩＣカードから暗号鍵媒介装置へ転送する。ステップ３３１１は、暗号鍵媒介装置から、暗号化した暗号鍵を受信側機器へ転送する。ステップ３３１２は、受信側機器が提示装置の場合で、暗号化した暗号鍵を共通鍵で解除して、番組を再生提示する。ステップ３３１３は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【０１３１】また、図２３，図２４の例と同様に、送信側機器から受信側機器へ暗号鍵媒介装置とＩＣカードの識別情報を送信して、暗号鍵媒介装置と受信側機器の認証に使用する方法も可能である。

【０１３２】以上により、送信側機器から暗号鍵媒介装置への暗号鍵の転送は、機器ごとに独自の仕様で暗号化を行い、暗号鍵媒介装置から、受信側機器への暗号鍵の転送には、ＩＣカードの識別情報を使用した提示装置ごとの共通鍵で暗号化する構成となり、暗号鍵の盗用を困難にすることができる。

【０１３３】図３５は、暗号鍵媒介装置に使用する機器を登録する場合の処理の流れ図を示す。また、図３６は、受信機と暗号鍵媒介装置、ＩＣカード、提示装置の間の処理シーケンスを示す。対応する処理に図３５と同じ番号が付されている。

【０１３４】ステップ３５０１は、使用する機器を暗号鍵媒介装置へ登録する。ステップ３５０２は、使用する機器を選択する。ステップ３５０３は、視聴または記録する番組を選択する。ステップ３５０４は、送信側機器が、選択した番組を暗号化する暗号鍵を暗号鍵媒介装置への登録情報に基づく共通鍵で暗号化する。ステップ３５０５は、暗号化した暗号鍵を暗号鍵媒介装置へ転送する。ステップ３５０６は、暗号鍵媒介装置が、送信側機器の登録情報に基づく共通鍵で暗号鍵の暗号を解除する。ステップ３５０７は、解除した暗号鍵をＩＣカードへ転送する。ステップ３５０８は、視聴時刻にＩＣカードから暗号鍵を暗号鍵媒介装置へ転送する。

【０１３５】ステップ３５０９は、暗号鍵を受信側機器の登録情報に基づく共通鍵で暗号化する。ステップ３５１０は、暗号鍵媒介装置と受信側機器がＩＣカードの識別情報などを使用して認証処理を行う。ステップ３５１１は、暗号化した暗号鍵を暗号鍵媒介装置から受信側機器へ転送する。ステップ３５１２は、受信側機器が提示装置の場合で、暗号鍵の暗号を解除して、番組の暗号を解除して再生提示する。ステップ３５１３は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【０１３６】以上により、あらかじめ登録した正規の機器と暗号鍵媒介装置との間では、共通鍵を生成して暗号鍵の受け渡しが行えるが、それ以外の機器との間では、暗号鍵の受け渡しが行えないため、違法な機器での視聴を防ぐことができる。

【０１３７】図３７は、暗号鍵媒介装置がリモコンなどを兼用して、提示装置と対になったＩＣカードを装着する形態の場合の処理の流れ図を示す。また、図３８は、受信機と暗号鍵媒介装置、ＩＣカード、提示装置の間の処理シーケンスを示す。対応する処理に図３７と同じ番号が付されている。

【０１３８】ステップ３７０１は、提示装置と対になったＩＣカードを暗号鍵媒介装置へ装着する。ステップ３７０２は、暗号鍵媒介装置とＩＣカードが認証処理を行う。ステップ３７０３は、視聴あるいは記録する番組を選択する。ステップ３７０４は、暗号鍵媒介装置が送信側機器を認証する。ステップ３７０５は、暗号鍵を送信側機器と暗号鍵媒介装置の間の専用の暗号化処理を行って、暗号鍵媒介装置へ転送する。

【０１３９】ステップ３７０６は、暗号鍵媒介装置が暗号鍵の暗号を解除する。ステップ３７０７は、解除した暗号鍵をＩＣカードへ転送する。ステップ３７０８は、ＩＣカードが暗号鍵を暗号化する。ステップ３７０９は、暗号鍵媒介装置と受信側機器が認証処理を行う。ステップ３７１０は、ＩＣカードが暗号化した暗号鍵を暗号鍵媒介装置へ転送する。ステップ３７１１は、暗号鍵

媒介装置が暗号化した暗号鍵を受信側機器へ転送する。ステップ３７１２は、受信側機器が提示装置の場合で、暗号化した暗号鍵を解除して、番組を再生提示する。ステップ３７１３は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【０１４０】以上により、送信側機器から暗号鍵媒介装置への暗号鍵の転送は、機器ごとに独自の仕様で暗号化を行い、暗号鍵媒介装置から、受信側機器への暗号鍵の転送には、ＩＣカードによる提示装置独自の暗号化を用いる構成となり、暗号鍵の盗用を困難にすることができる。

【０１４１】図３９は、提示装置に入力装置、または入力装置の接続部が備えられている場合の処理の流れ図を示す。また、図４０は、受信機と暗号鍵媒介装置、提示装置、記録手段の間の処理シーケンスを示す。対応する処理に図３９と同じ番号が付されている。

【０１４２】ステップ３９０１は、提示装置上で、使用する機器の選択を行う。ステップ３９０２は、提示装置と選択した使用機器の間で認証を行う。ステップ３９０３は，選択した送信側機器から番組情報リストを提示装置へ転送する。ステップ３９０４は、視聴あるいは記録する番組を選択する。

【０１４３】ステップ３９０５は、提示装置から番組選択情報を暗号化して、選択した送信側機器へ転送する。ステップ３９０６は、送信側機器から暗号化した暗号鍵を暗号鍵媒介手段へ電波などで転送する。ステップ３９０７は、暗号鍵媒介装置が暗号化した暗号鍵を解除する。ステップ３９０８は、暗号鍵媒介装置が暗号鍵を暗号化して提示装置へ転送する。ステップ３９０９は、提示装置が暗号鍵の暗号を解除して、番組を再生する。

【０１４４】ステップ３９１０は、記録する場合には、提示装置が解除した暗号鍵を暗号化して記録装置へ転送する。ステップ３９１１は、記録装置が暗号化した暗号鍵をそのまま記録する。

【０１４５】以上により、暗号鍵媒介装置への情報の入力は、送信側機器からのみとなり、暗号鍵媒介装置からの出力は、提示装置へだけとなり、インターフェースが単純になる。

【０１４６】図４１は、自己録再の番組あるいは、著作権保護に関する制限が無いまたは、編集を許可された番組がある場合の処理の流れ図を示す。

【０１４７】ステップ４１０１は、視聴または、記録、編集する番組を選択する。ステップ４１０２は、自己録再の番組かどうかを判定する。ステップ４１０３は、自作の番組ではない場合で、著作権保護に関する制限がないかどうかを判定する。ステップ４１０４は、著作権保護に関する制限がある場合で、編集が許可されているかどうかを判定する。

【０１４８】ステップ４１０５は、自己録再の番組または、著作権保護に関する制限がない場合または、編集が許可されている場合で、暗号化しないで、番組を出力する。ステップ４１０６は、暗号化されていない番組を提示手段が提示する。あるいは、記録手段などで、記録、編集を行う。

【０１４９】ステップ４１０７は、編集が許可されていない場合で、選択した番組を暗号化して出力する。ステップ４１０８は、提示手段で暗号を解除して提示、または、記録が許可されている時には記録手段で記録する。ステップ４１０７、４１０８の具体的な処理は、図３０のステップ３００３以降の処理になる。

【０１５０】以上により、著作権保護に関する制限が無いコンテンツなどは、自由に編集作業を行うことができる。

【０１５１】本発明の実施の形態では、ＭＰＥＧのコンテンツを暗号化してディスプレイやスピーカへ出力し、ディスプレイ、スピーカで暗号を解除し、ＭＰＥＧデコードして直接再生するといったことを行うため、暗号化を解除された状態では機器の外部には出力されない。また、暗号鍵も別に暗号化して、コンテンツとは別の系統で送受信し、送信側機器と暗号鍵媒介装置と受信側機器の３者で正常に認証を行った場合にのみ暗号鍵が受信側の機器に渡るため、違法にコピーされても再生することが非常に困難になる。

【０１５２】

【発明の効果】本発明によれば、著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態の構成のブロック図を示す。

【図２】図１の受信機１０１の実施の形態の構成のブロック図を示す。

【図３】図１の提示装置１０５の第１の実施の形態の構成のブロック図を示す。

【図４】図１の記録装置１０２の第１の実施の形態の構成のブロック図を示す。

【図５】図１の再生装置１０３の第１の実施の形態の構成のブロック図を示す。

【図６】図１のコンピュータ１０３の第１の実施の形態の構成のブロック図を示す。

【図７】図１の提示装置１０５の第２の実施の形態の構成のブロック図を示す。

【図８】暗号鍵媒介装置の第１の実施の形態の構成のブロック図を示す。

【図９】暗号鍵媒介装置の第２の実施の形態の構成のブロック図を示す。

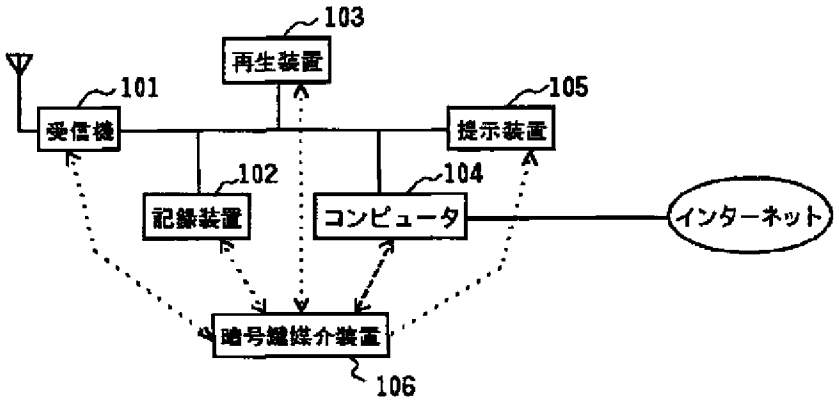
【図１０】暗号鍵媒介装置の第３の実施の形態の構成のブロック図を示す。

【図１１】暗号鍵媒介装置の第４の実施の形態の構成の

ブロック図を示す。
【図１２】図１１の認証手段１１０２の構成のブロック図を示す。
【図１３】暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の認証手段の第１の実施の形態の構成のブロック図を示す。
【図１４】暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の第２の実施の形態の構成のブロック図を示す。
【図１５】暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の第３の実施の形態の構成のブロック図を示す。
【図１６】暗号鍵媒介装置と第１のデジタルメディア機器，第２のデジタルメディア機器の認証手段の第４実施の形態の構成のブロック図を示す。
【図１７】暗号鍵媒介装置の他の構成を示す図である。
【図１８】暗号鍵媒介装置の別の実施の形態の構成のブロック図を示す。
【図１９】暗号鍵媒介装置のさらに別の実施の形態の構成のブロック図を示す。
【図２０】暗号鍵媒介装置のさらに別の実施の形態の構成のブロック図を示す。
【図２１】機器を認証して暗号鍵を転送する処理の流れ図を示す。
【図２２】図２１の処理シーケンスを示す図である。
【図２３】暗号鍵媒介装置と機器の認証処理だけの流れ図を示す。
【図２４】図２３の処理シーケンスを示す図である。
【図２５】暗号鍵を送信側機器から受信側機器へ転送する処理だけの流れ図を示す。
【図２６】図２５の処理シーケンスを示す図である。
【図２７】暗号鍵媒介装置として、送信側機器と受信側機器を直接接続する形態をとる場合の認証と暗号鍵の転送処理の流れ図を示す。
【図２８】ＰＣなどのコンピュータへ出力する場合の処理の流れ図を示す。
【図２９】ＰＣなどのコンピュータが送信側機器になった場合に視聴する処理の流れ図を示す。
【図３０】記録に制限がある場合を含めた処理の流れ図を示す。
【図３１】記録に制限がある場合を含めた処理の流れ図を示す。
【図３２】記録に制限がある場合を含めた処理の流れ図を示す。
【図３３】暗号鍵媒介装置がリモコンなどを兼用して、ＩＣカードを装着する形態の場合の処理の流れ図を示す。
【図３４】図３３の処理シーケンスを示す図である。
【図３５】暗号鍵媒介装置に使用する機器を登録する場合の処理の流れ図を示す。
【図３６】図３５の処理シーケンスを示す図である。
【図３７】暗号鍵媒介装置がリモコンなどを兼用して、ＩＣカードを装着する形態の場合の処理の流れ図を示す。
【図３８】図３７の処理シーケンスを示す図である。
【図３９】提示装置に入力装置、または入力装置の接続部が備えられている場合の処理の流れ図を示す。
【図４０】図３９の処理シーケンスを示す図である。
【図４１】著作権保護に関する制限がある場合と無い場合を含めた処理の流れ図を示す。
【符号の説明】
１０１…受信機、１０２…記録装置、１０３…再生装置、１０４…コンピュータ、１０５…提示装置、１０６…暗号鍵媒介装置、２０１…復調手段、２０２…誤り訂正手段、２０３…デスクランブル手段、２０４…分離手段、２０５，５０３…暗号化手段、２０６，３０１，４０１，５０１，６０１，１１０２…認証手段、２０７，５０２，１１０１…暗号鍵生成手段、３０２…暗号解除手段、３０３…復号手段、３０４…映像再生手段、３０５…音声再生手段、４０２…暗号鍵用暗号鍵生成手段、４０３…暗号鍵暗号化復号化手段、４０４…記録装置、５０４…記録媒体、６０２…演算装置、６０３…記憶装置、６０４…映像音声変換装置、７０１…入力先判定手段、７０２…入力手段、８０１…暗号鍵熱変換手段、８０２…熱暗号鍵検出手段、９０１…暗号鍵振動変換手段、９０２…振動暗号鍵検出手段、１００１…暗号鍵磁界変換手段、１００２…抵抗暗号鍵検出手段、１１０３…乱数発生手段、１１０４…記憶手段、１１０５…暗号化復号化手段、１２０１…提示手段、１２０２…認識手段、１２０３…変換手段、１２０４…処理部、１３０１…認証部、１３０２…揮発性光学メモリ、１３０３…シャッター部、１３０４…受光部、１３０５…発光部、１３０６、１４０３、１５０２、１６０２…暗号鍵変換部、１４０１…記録部、１４０２…温度感応発生部、１５０１…圧力感応発生部、１６０１…超音波発生受信部、１７０１…可動導体、１７０２…接点、１８０１…ＩＣカード、１８０２…ＩＣカード認証手段、１８０３…暗号化復号化手段、１８０４…機器認証手段、１８０５…電磁波送受信手段、１９０１…機器登録手段、２００１…暗号化ＩＣカード、２００２…暗号鍵復号手段。

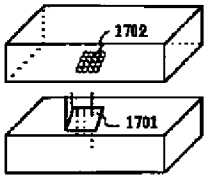
【図１】

図 1



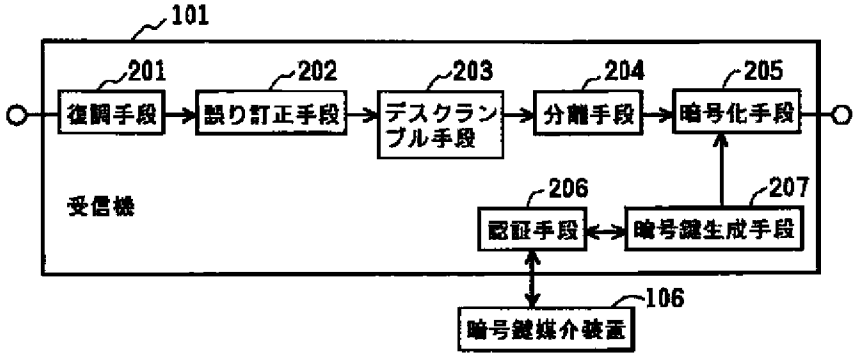
【図１７】

図 17



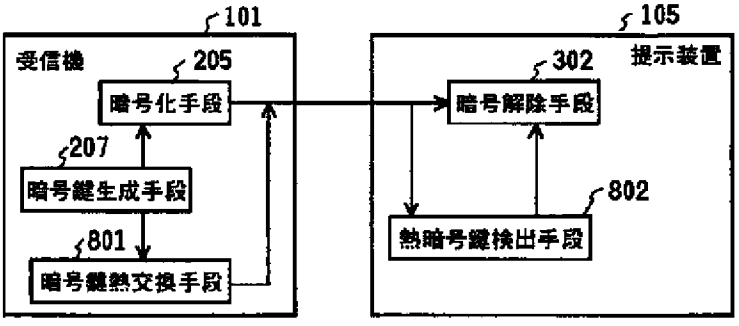
【図２】

図 2



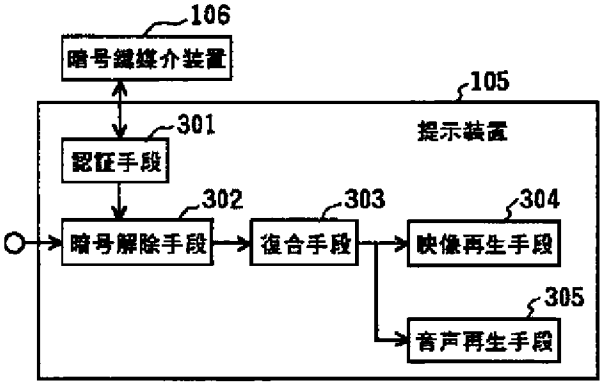
【図８】

図 8



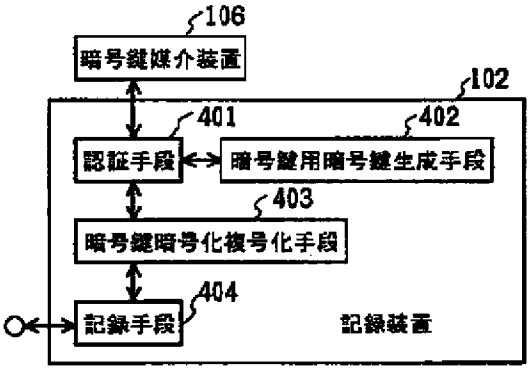
【図３】

図　3



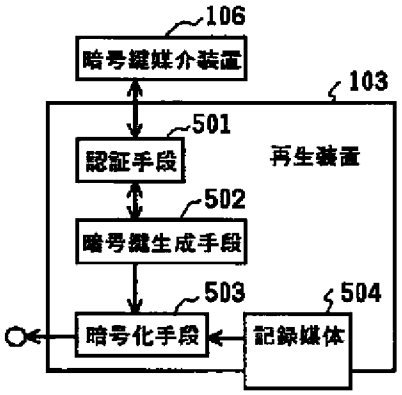
【図４】

図　4



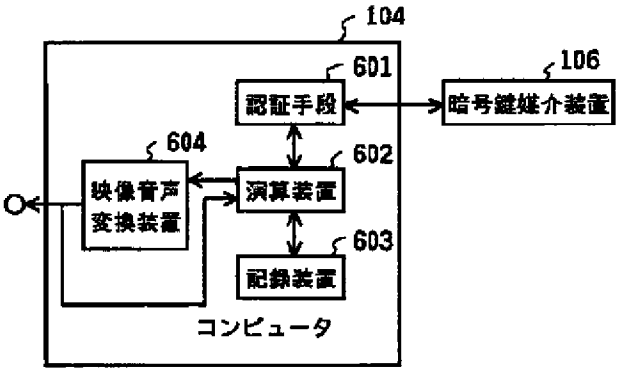
【図５】

図　5



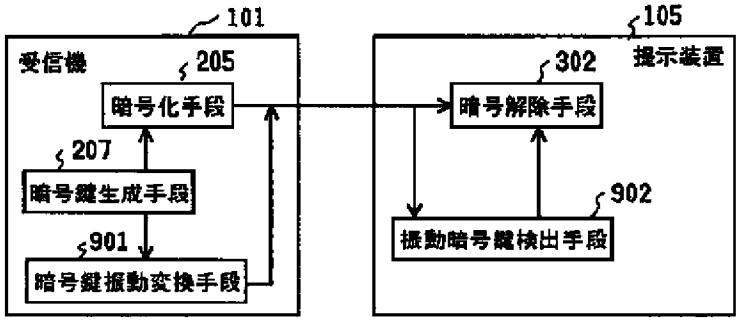
【図６】

図　6



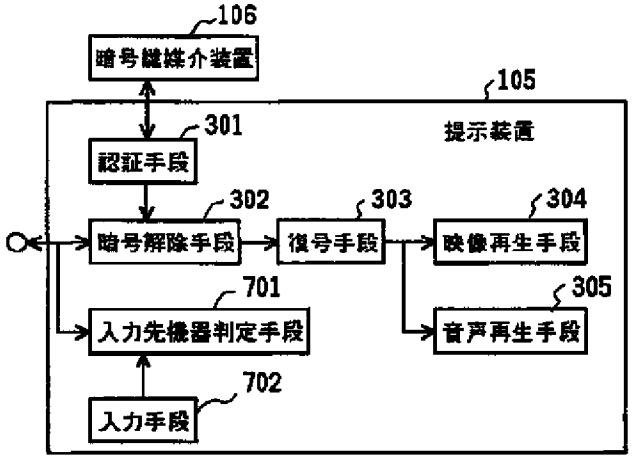
【図９】

図　9



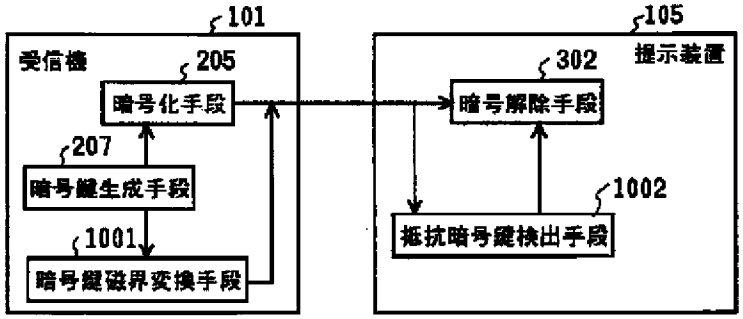
【図７】

図 7



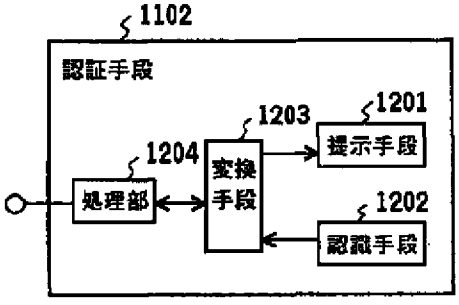
【図１０】

図 10



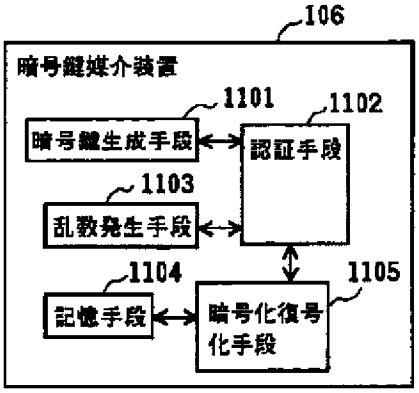
【図１２】

図 12



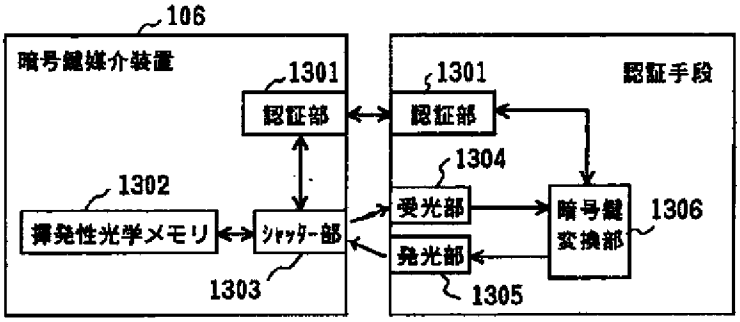
【図１１】

図 11



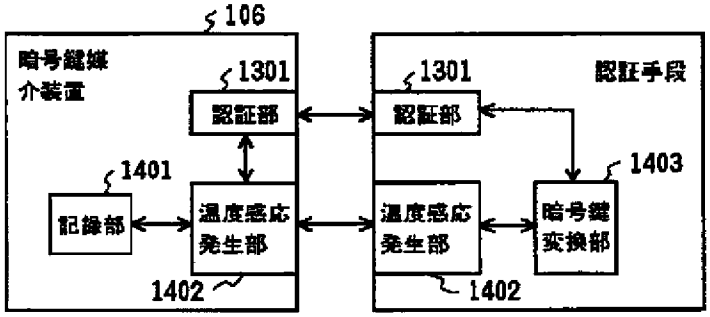
【図１３】

図　13



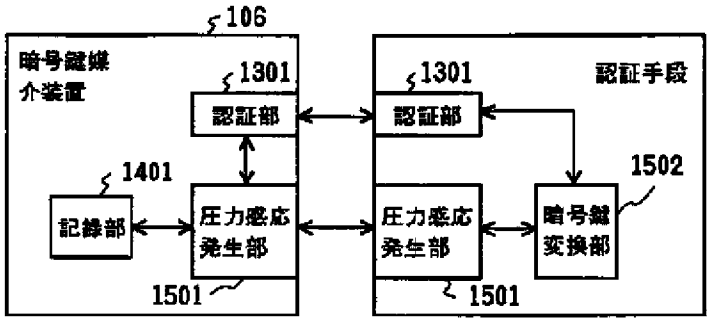
【図１４】

図　14



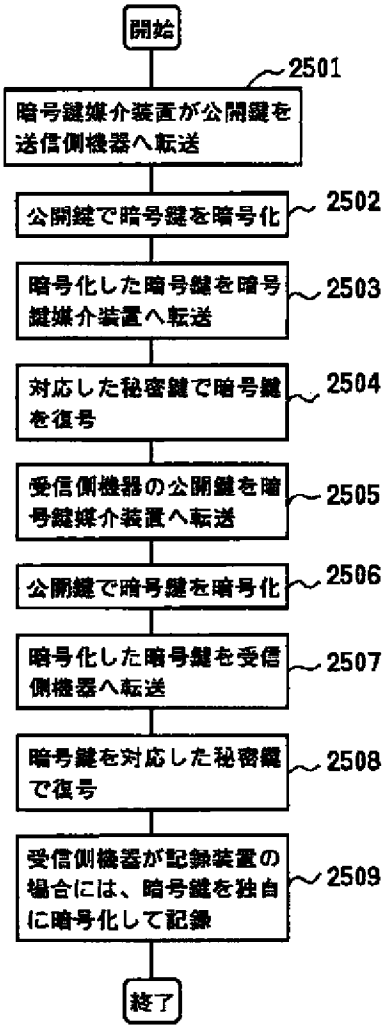
【図１５】

図　15



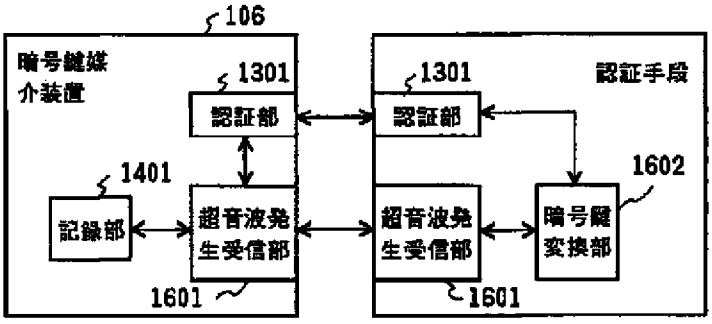
【図２５】

図　25



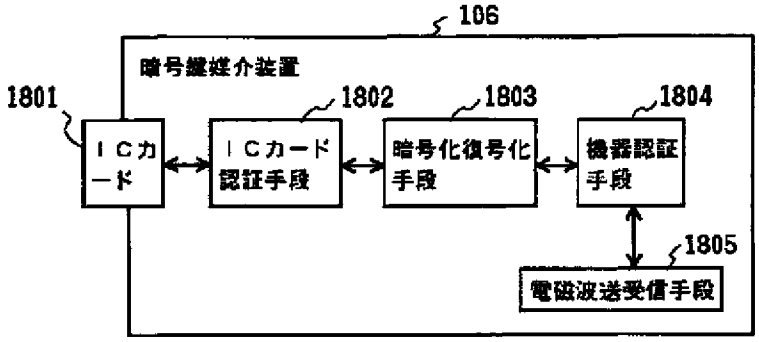
【図１６】

図 16



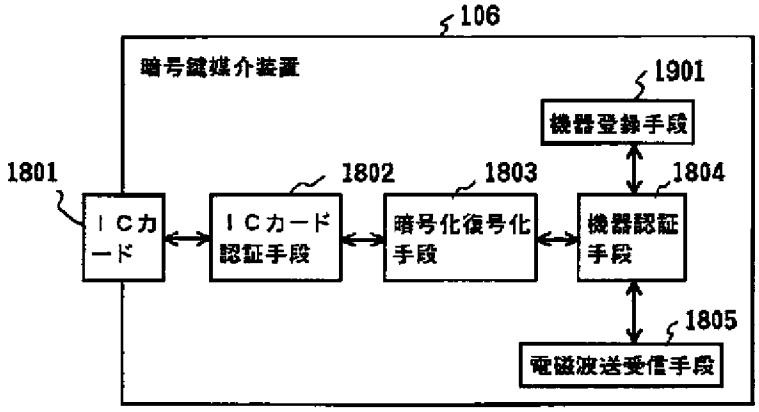
【図１８】

図 18



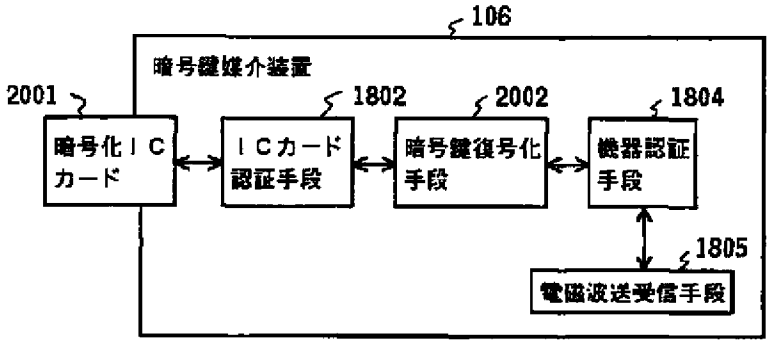
【図１９】

図 19



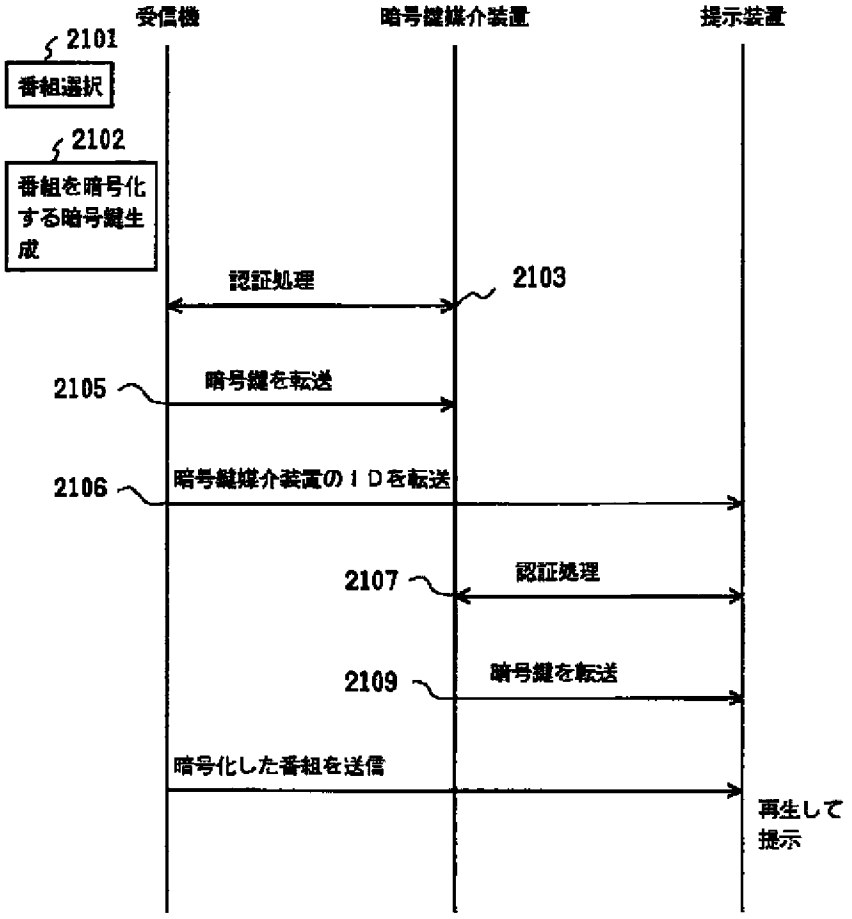
【図２０】

図 20



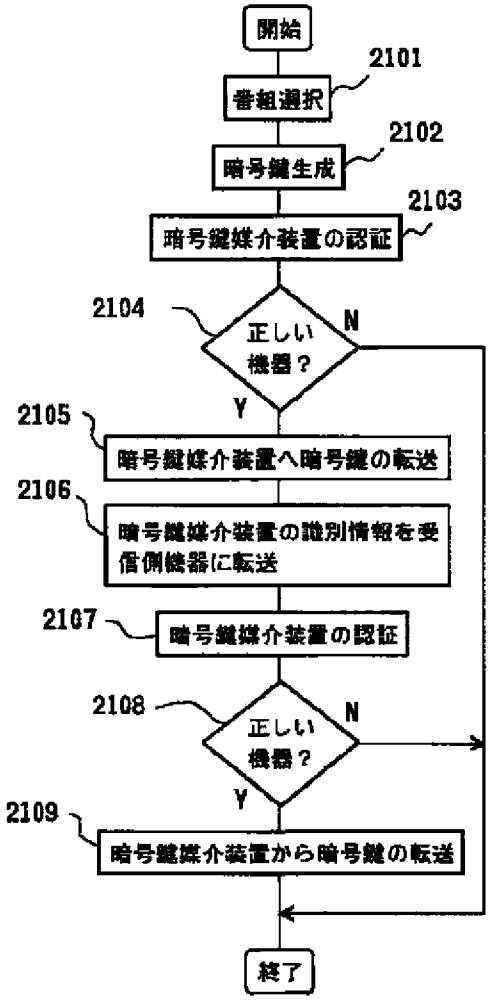
【図２２】

図 22



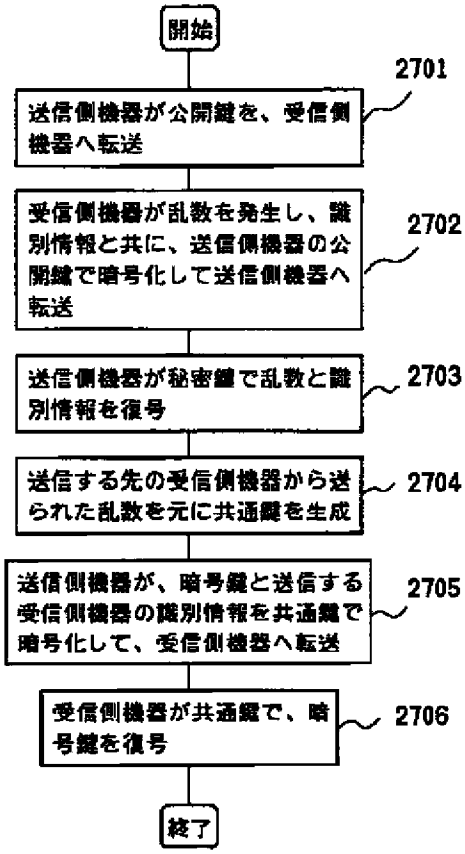
【図２１】

図 21



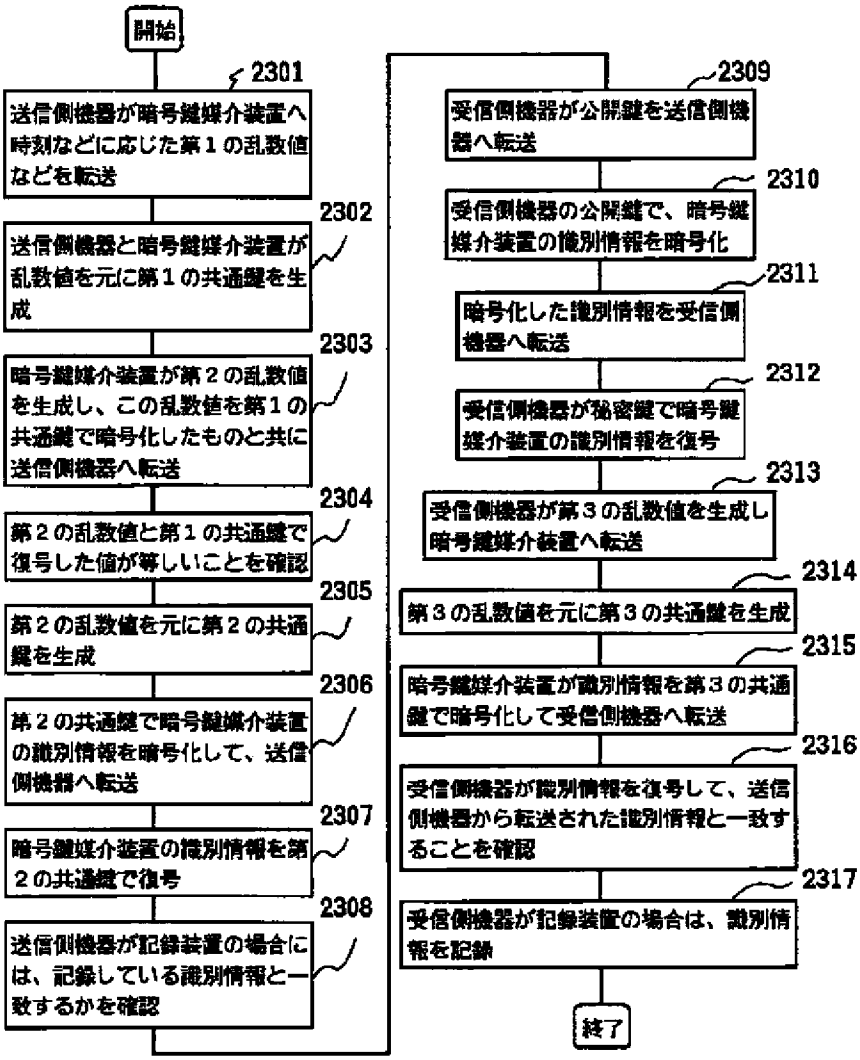
【図２７】

図 27



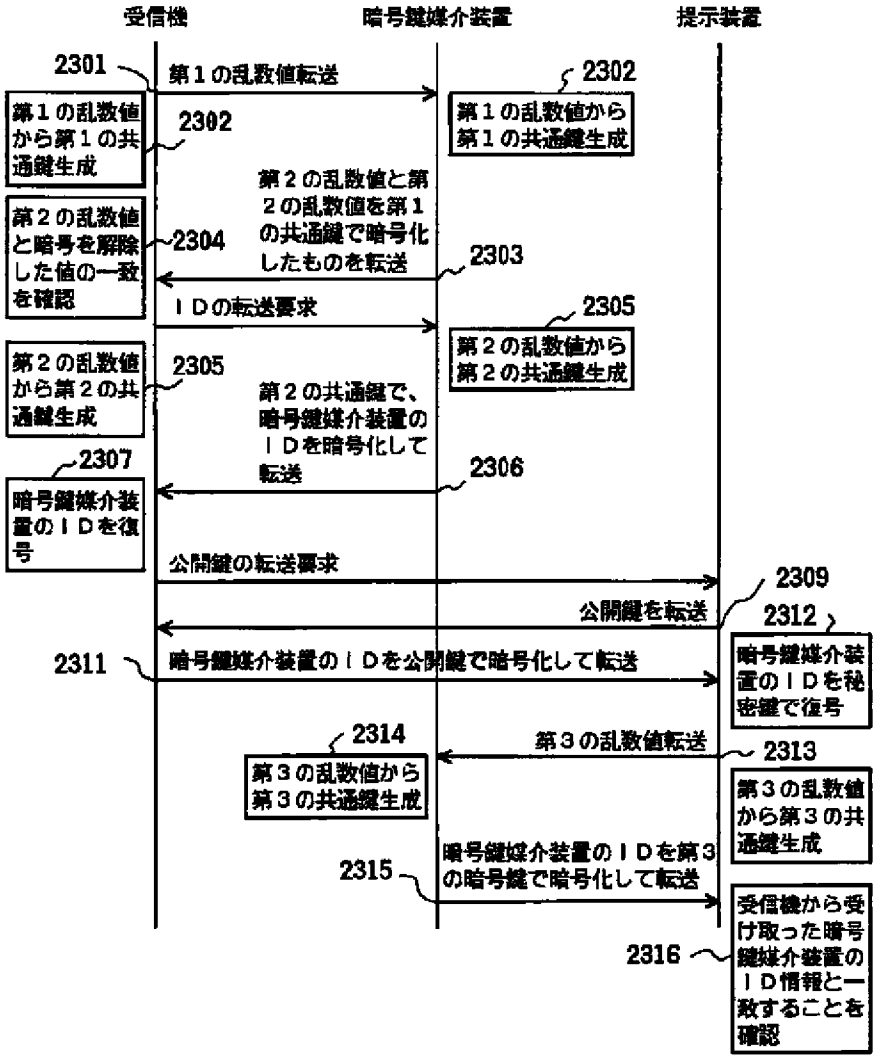
【図２３】

図 23


開始
2301
送信側機器が暗号鍵媒介装置へ時刻などに応じた第１の乱数値などを転送
2302
送信側機器と暗号鍵媒介装置が乱数値を元に第１の共通鍵を生成
2303
暗号鍵媒介装置が第２の乱数値を生成し、この乱数値を第１の共通鍵で暗号化したものと共に送信側機器へ転送
2304
第２の乱数値と第１の共通鍵で復号した値が等しいことを確認
2305
第２の乱数値を元に第２の共通鍵を生成
2306
第２の共通鍵で暗号鍵媒介装置の識別情報を暗号化して、送信側機器へ転送
2307
暗号鍵媒介装置の識別情報を第２の共通鍵で復号
2308
送信側機器が記録装置の場合には、記録している識別情報と一致するかを確認
2309
受信側機器が公開鍵を送信側機器へ転送
2310
受信側機器の公開鍵で、暗号鍵媒介装置の識別情報を暗号化
2311
暗号化した識別情報を受信側機器へ転送
2312
受信側機器が秘密鍵で暗号鍵媒介装置の識別情報を復号
2313
受信側機器が第３の乱数値を生成し暗号鍵媒介装置へ転送
2314
第３の乱数値を元に第３の共通鍵を生成
2315
暗号鍵媒介装置が識別情報を第３の共通鍵で暗号化して受信側機器へ転送
2316
受信側機器が識別情報を復号して、送信側機器から転送された識別情報と一致することを確認
2317
受信側機器が記録装置の場合は、識別情報を記録
終了

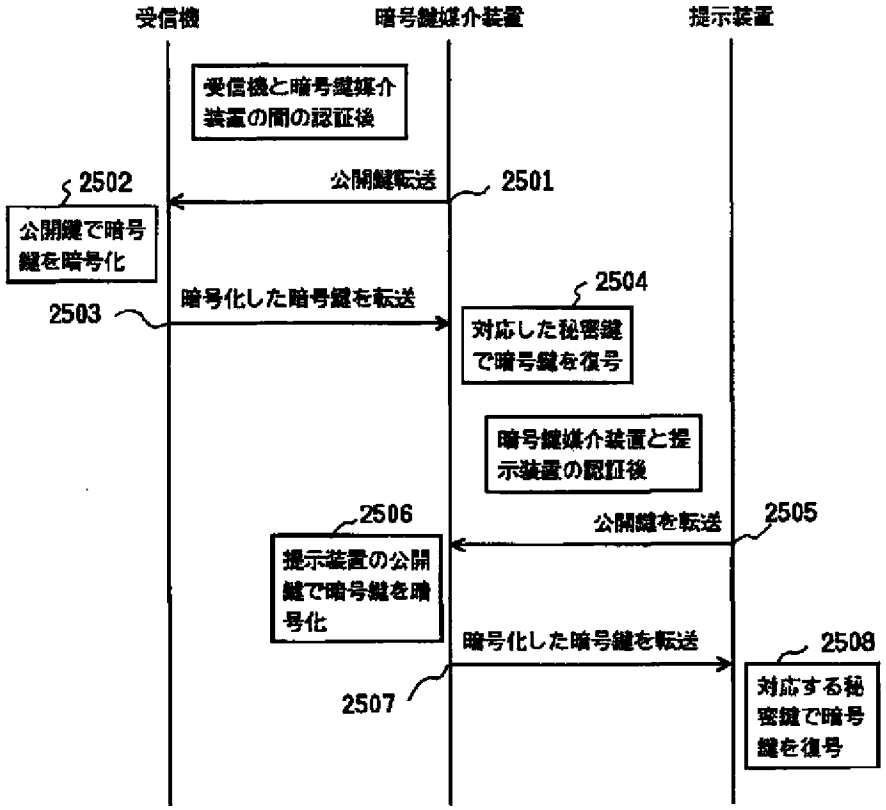
【図２４】

図　24


受信機
暗号鍵媒介装置
提示装置
2301
第１の乱数値転送
2302
第１の乱数値から第１の共通鍵生成
第１の乱数値から第１の共通鍵生成
2302
第２の乱数値と第２の乱数値を第１の共通鍵で暗号化したものを転送
2303
第２の乱数値と暗号を解除した値の一致を確認
2304
ＩＤの転送要求
2305
第２の乱数値から第２の共通鍵生成
第２の乱数値から第２の共通鍵生成
2305
第２の共通鍵で、暗号鍵媒介装置のＩＤを暗号化して転送
2306
暗号鍵媒介装置のＩＤを復号
2307
公開鍵の転送要求
公開鍵を転送
2309
暗号鍵媒介装置のＩＤを秘密鍵で復号
2312
暗号鍵媒介装置のＩＤを公開鍵で暗号化して転送
2311
第３の乱数値転送
2313
第３の乱数値から第３の共通鍵生成
2314
第３の乱数値から第３の共通鍵生成
暗号鍵媒介装置のＩＤを第３の暗号鍵で暗号化して転送
2315
受信機から受け取った暗号鍵媒介装置のＩＤ情報と一致することを確認
2316

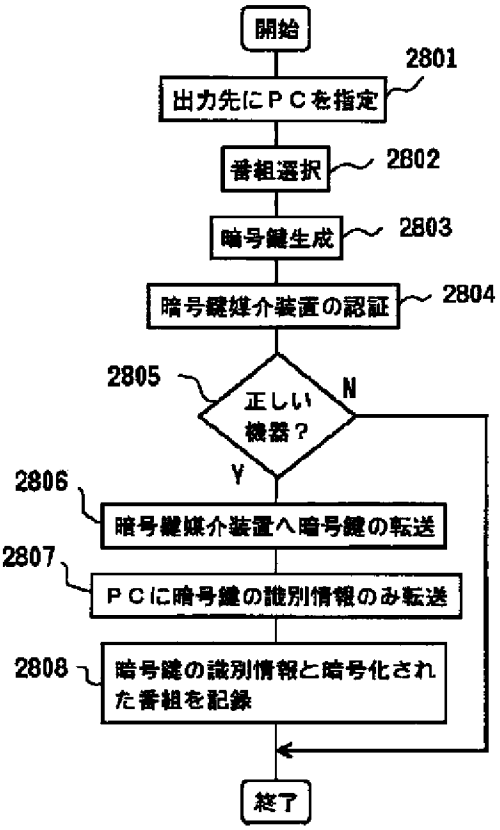
【図２６】

図 26


受信機
暗号鍵媒介装置
提示装置
受信機と暗号鍵媒介装置の間の認証後
2502
公開鍵転送
2501
公開鍵で暗号鍵を暗号化
暗号化した暗号鍵を転送
2503
2504
対応した秘密鍵で暗号鍵を復号
暗号鍵媒介装置と提示装置の認証後
2506
公開鍵を転送
2505
提示装置の公開鍵で暗号鍵を暗号化
暗号化した暗号鍵を転送
2508
2507
対応する秘密鍵で暗号鍵を復号

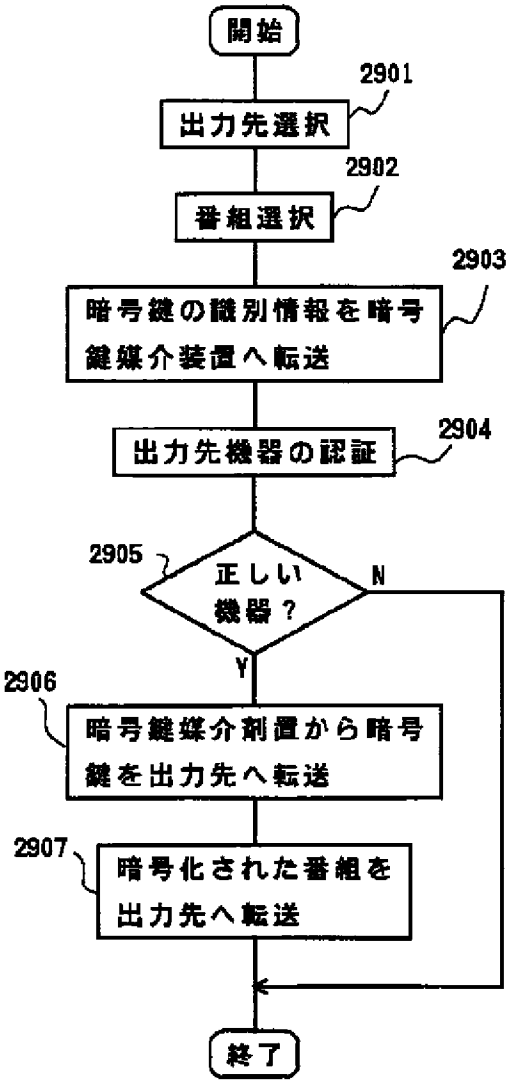
【図２８】

図 28



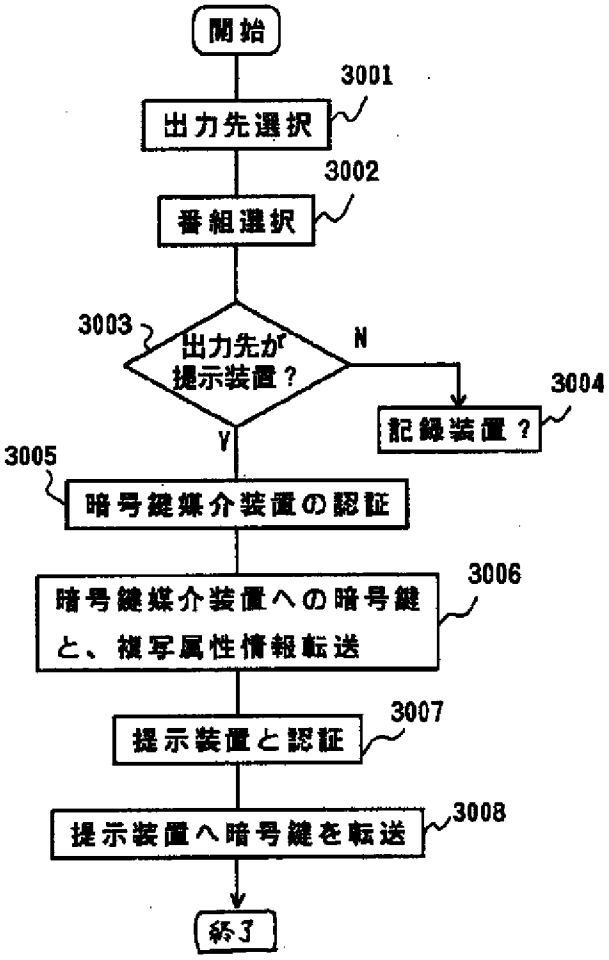
【図２９】

図 29



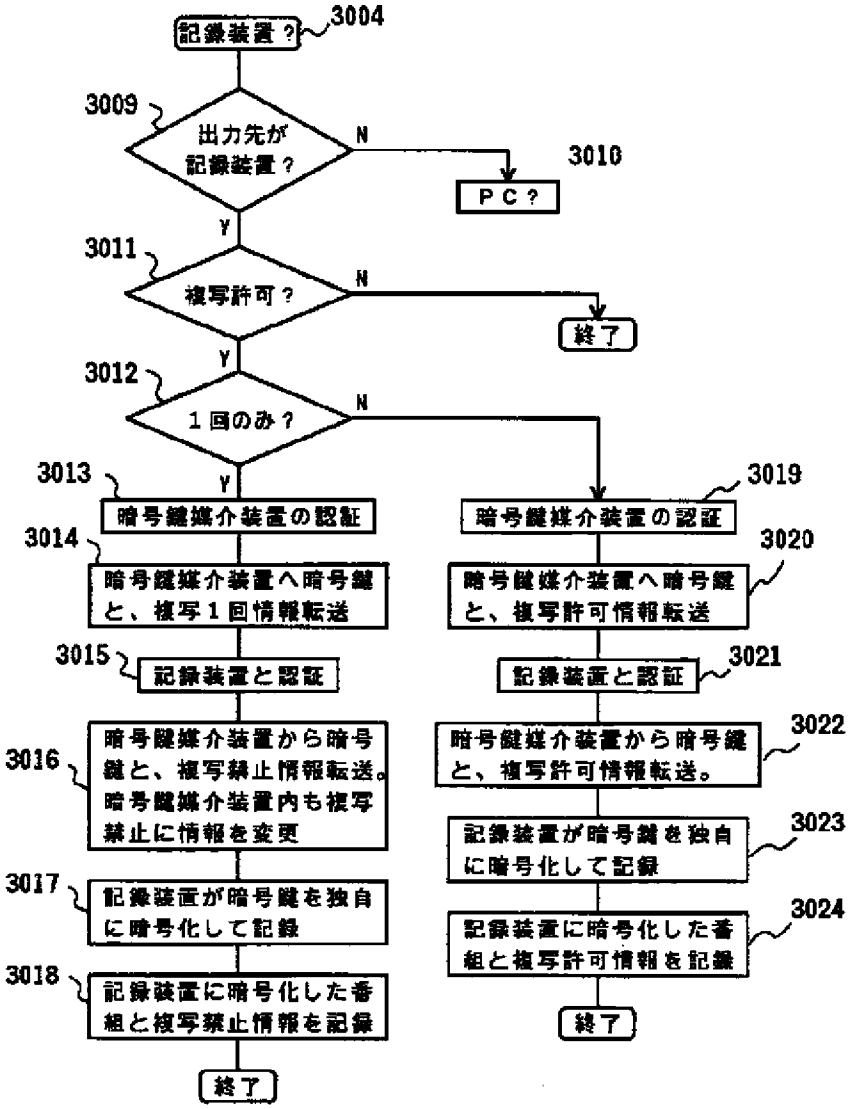
【図30】

図 30


開始
3001
出力先選択
3002
番組選択
3003
出力先が提示装置？
N
3004
記録装置？
Y
3005
暗号鍵媒介装置の認証
3006
暗号鍵媒介装置への暗号鍵と、複写属性情報転送
3007
提示装置と認証
3008
提示装置へ暗号鍵を転送
終了

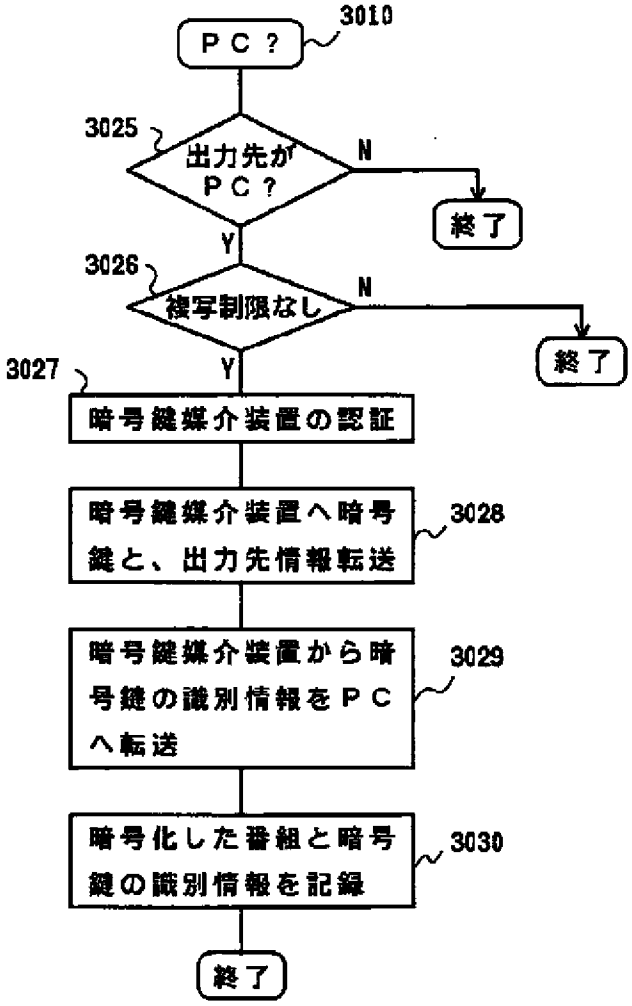
【図３１】

図 31


記録装置？
3004
3009
出力先が記録装置？
N
3010
PC？
Y
3011
複写許可？
N
終了
Y
3012
１回のみ？
N
Y
3013
暗号鍵媒介装置の認証
3014
暗号鍵媒介装置へ暗号鍵と、複写１回情報転送
3015
記録装置と認証
3016
暗号鍵媒介装置から暗号鍵と、複写禁止情報転送。暗号鍵媒介装置内も複写禁止に情報を変更
3017
記録装置が暗号鍵を独自に暗号化して記録
3018
記録装置に暗号化した番組と複写禁止情報を記録
終了
3019
暗号鍵媒介装置の認証
3020
暗号鍵媒介装置へ暗号鍵と、複写許可情報転送
3021
記録装置と認証
3022
暗号鍵媒介装置から暗号鍵と、複写許可情報転送。
3023
記録装置が暗号鍵を独自に暗号化して記録
3024
記録装置に暗号化した番組と複写許可情報を記録
終了

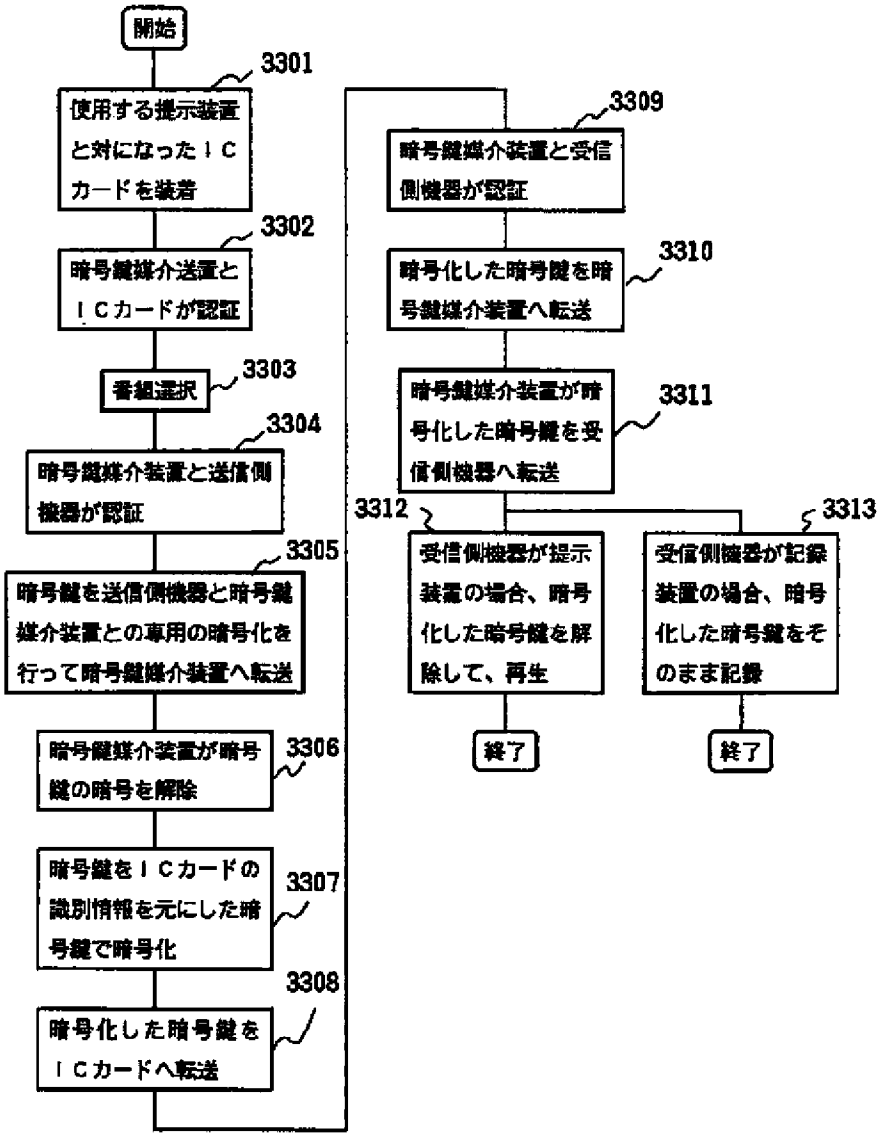
【図３２】

図 32


３０１０
ＰＣ？
３０２５
出力先がＰＣ？
N
終了
Y
３０２６
複写制限なし
N
終了
Y
３０２７
暗号鍵媒介装置の認証
暗号鍵媒介装置へ暗号鍵と、出力先情報転送
３０２８
暗号鍵媒介装置から暗号鍵の識別情報をＰＣへ転送
３０２９
暗号化した番組と暗号鍵の識別情報を記録
３０３０
終了

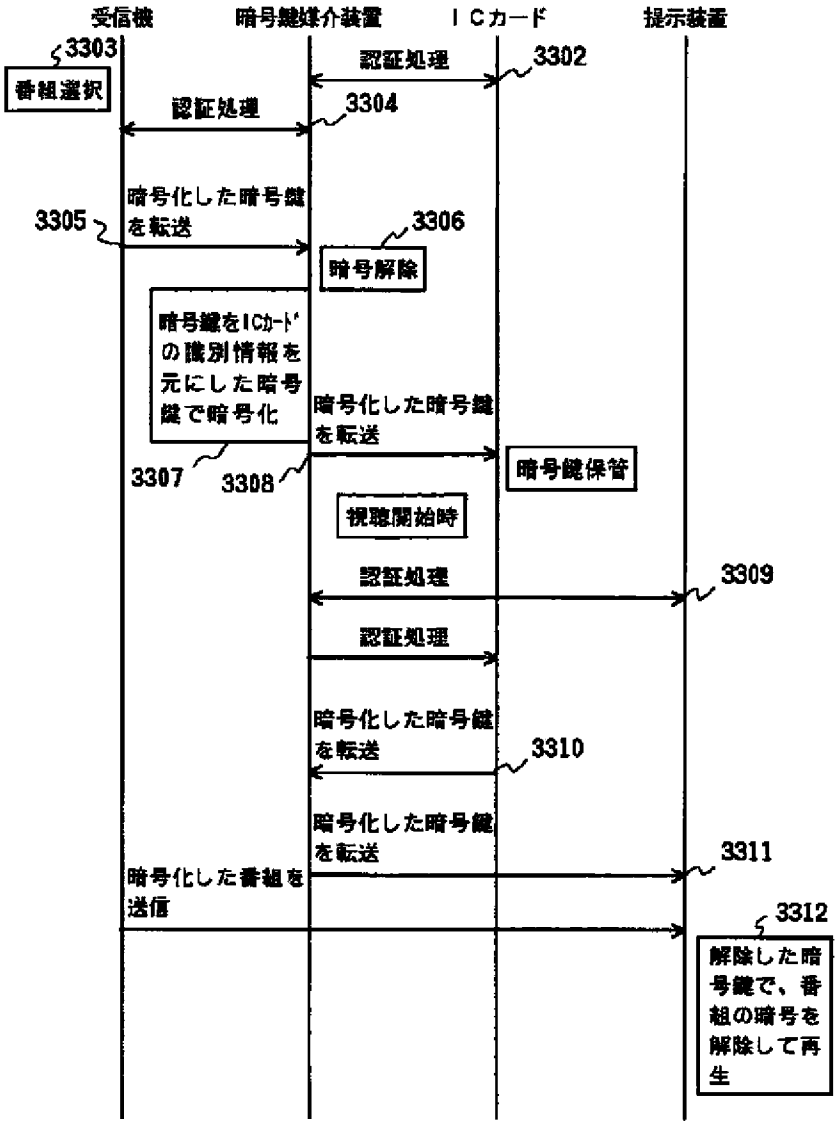
【図３３】

図　33


開始
3301
使用する提示装置と対になったＩＣカードを装着
3302
暗号鍵媒介装置とＩＣカードが認証
3303
番組選択
3304
暗号鍵媒介装置と送信側機器が認証
3305
暗号鍵を送信側機器と暗号鍵媒介装置との専用の暗号化を行って暗号鍵媒介装置へ転送
3306
暗号鍵媒介装置が暗号鍵の暗号を解除
3307
暗号鍵をＩＣカードの識別情報を元にした暗号鍵で暗号化
3308
暗号化した暗号鍵をＩＣカードへ転送
3309
暗号鍵媒介装置と受信側機器が認証
3310
暗号化した暗号鍵を暗号鍵媒介装置へ転送
3311
暗号鍵媒介装置が暗号化した暗号鍵を受信側機器へ転送
3312
受信側機器が提示装置の場合、暗号化した暗号鍵を解除して、再生
3313
受信側機器が記録装置の場合、暗号化した暗号鍵をそのまま記録
終了
終了

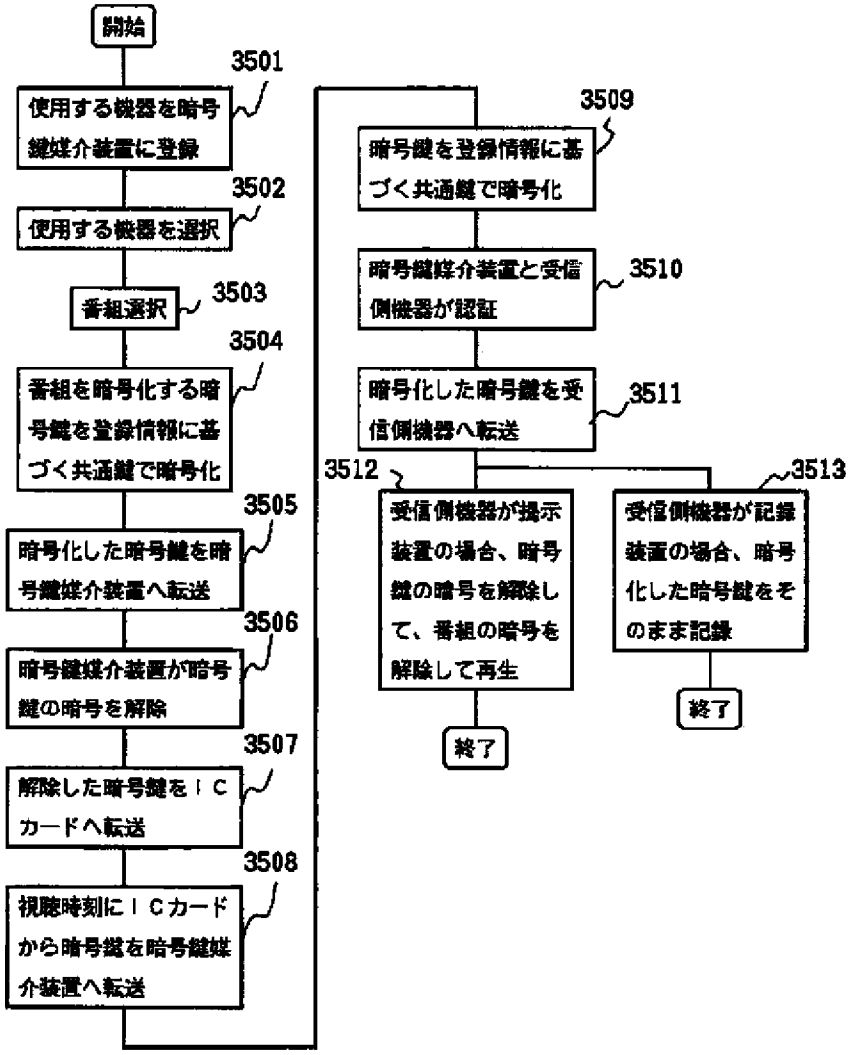
【図３４】

図 34


受信機
暗号鍵媒介装置
ＩＣカード
提示装置
3303
番組選択
認証処理
3302
認証処理
3304
暗号化した暗号鍵を転送
3305
3306
暗号解除
暗号鍵をICカードの識別情報を元にした暗号鍵で暗号化
暗号化した暗号鍵を転送
3307
3308
暗号鍵保管
視聴開始時
認証処理
3309
認証処理
暗号化した暗号鍵を転送
3310
暗号化した暗号鍵を転送
3311
暗号化した番組を送信
3312
解除した暗号鍵で、番組の暗号を解除して再生

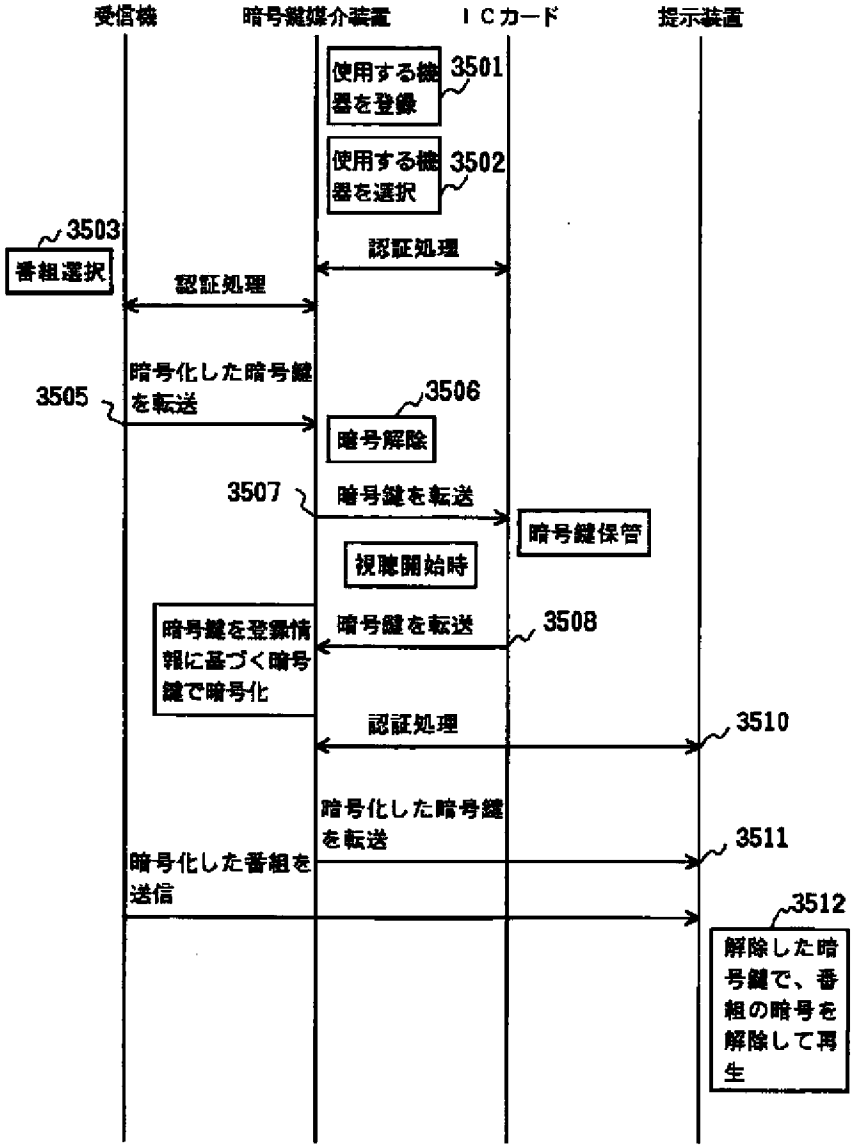
【図３５】

図 35


開始
3501
使用する機器を暗号鍵媒介装置に登録
3502
使用する機器を選択
番組選択
3503
3504
番組を暗号化する暗号鍵を登録情報に基づく共通鍵で暗号化
3505
暗号化した暗号鍵を暗号鍵媒介装置へ転送
3506
暗号鍵媒介装置が暗号鍵の暗号を解除
3507
解除した暗号鍵をＩＣカードへ転送
3508
視聴時刻にＩＣカードから暗号鍵を暗号鍵媒介装置へ転送
3509
暗号鍵を登録情報に基づく共通鍵で暗号化
3510
暗号鍵媒介装置と受信側機器が認証
3511
暗号化した暗号鍵を受信側機器へ転送
3512
受信側機器が提示装置の場合、暗号鍵の暗号を解除して、番組の暗号を解除して再生
終了
3513
受信側機器が記録装置の場合、暗号化した暗号鍵をそのまま記録
終了

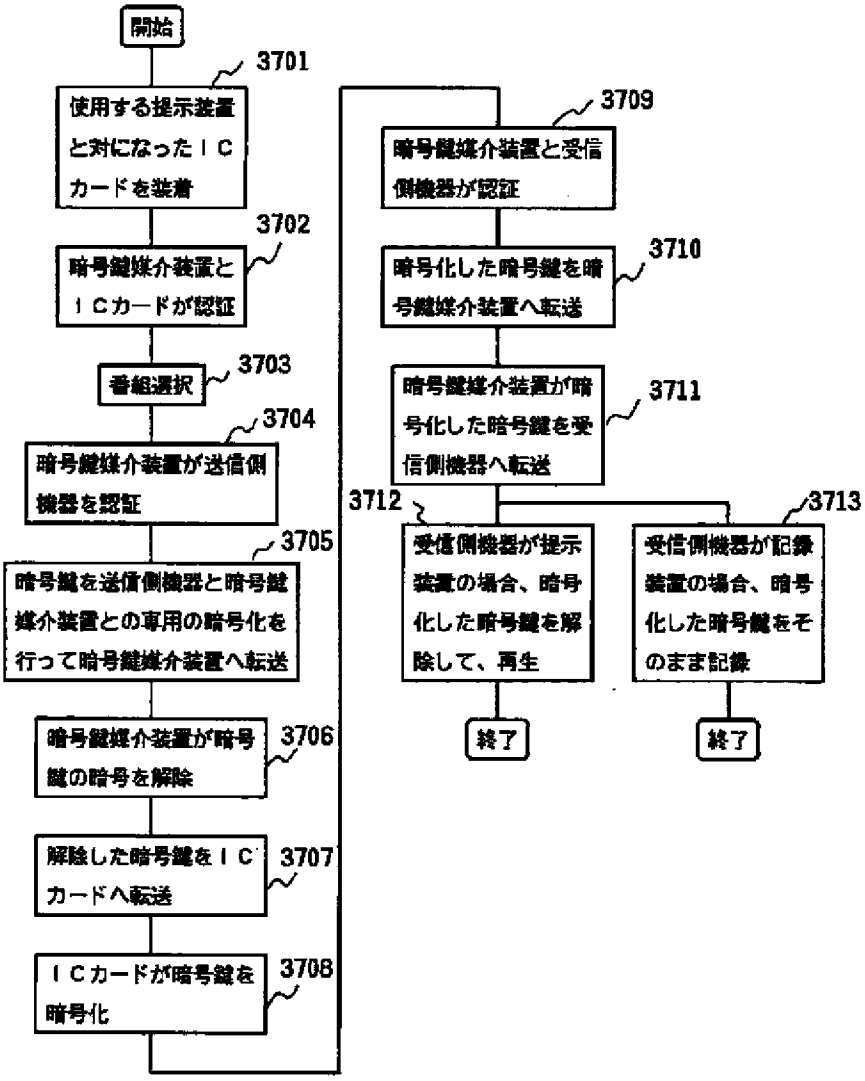
【図３６】

図 36


受信機
暗号鍵媒介装置
ＩＣカード
提示装置
使用する機器を登録
3501
使用する機器を選択
3502
3503
番組選択
認証処理
認証処理
暗号化した暗号鍵を転送
3505
3506
暗号解除
3507
暗号鍵を転送
暗号鍵保管
視聴開始時
暗号鍵を登録情報に基づく暗号鍵で暗号化
暗号鍵を転送
3508
認証処理
3510
暗号化した暗号鍵を転送
3511
暗号化した番組を送信
3512
解除した暗号鍵で、番組の暗号を解除して再生

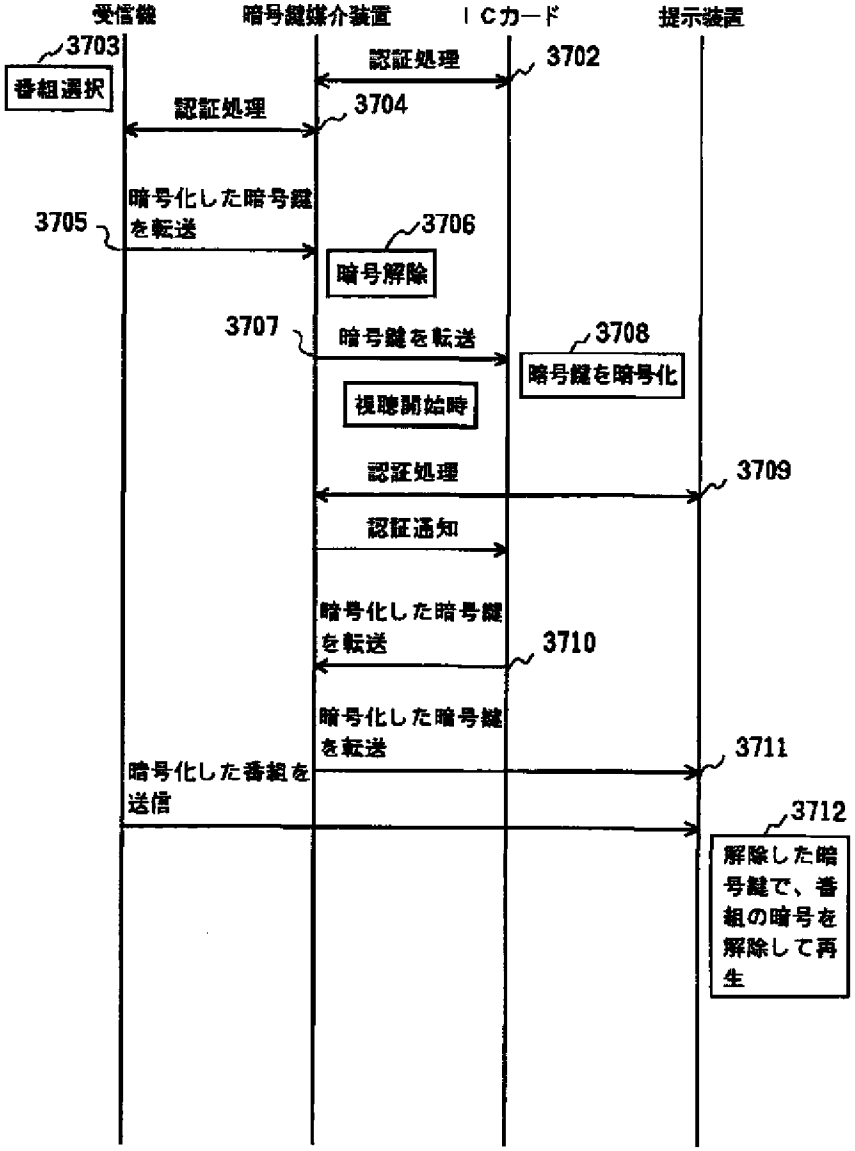
【図３７】

図 37


開始
3701
使用する提示装置と対になったＩＣカードを装着
3702
暗号鍵媒介装置とＩＣカードが認証
3703
番組選択
3704
暗号鍵媒介装置が送信側機器を認証
3705
暗号鍵を送信側機器と暗号鍵媒介装置との専用の暗号化を行って暗号鍵媒介装置へ転送
3706
暗号鍵媒介装置が暗号鍵の暗号を解除
3707
解除した暗号鍵をＩＣカードへ転送
3708
ＩＣカードが暗号鍵を暗号化
3709
暗号鍵媒介装置と受信側機器が認証
3710
暗号化した暗号鍵を暗号鍵媒介装置へ転送
3711
暗号鍵媒介装置が暗号化した暗号鍵を受信側機器へ転送
3712
受信側機器が提示装置の場合、暗号化した暗号鍵を解除して、再生
3713
受信側機器が記録装置の場合、暗号化した暗号鍵をそのまま記録
終了
終了

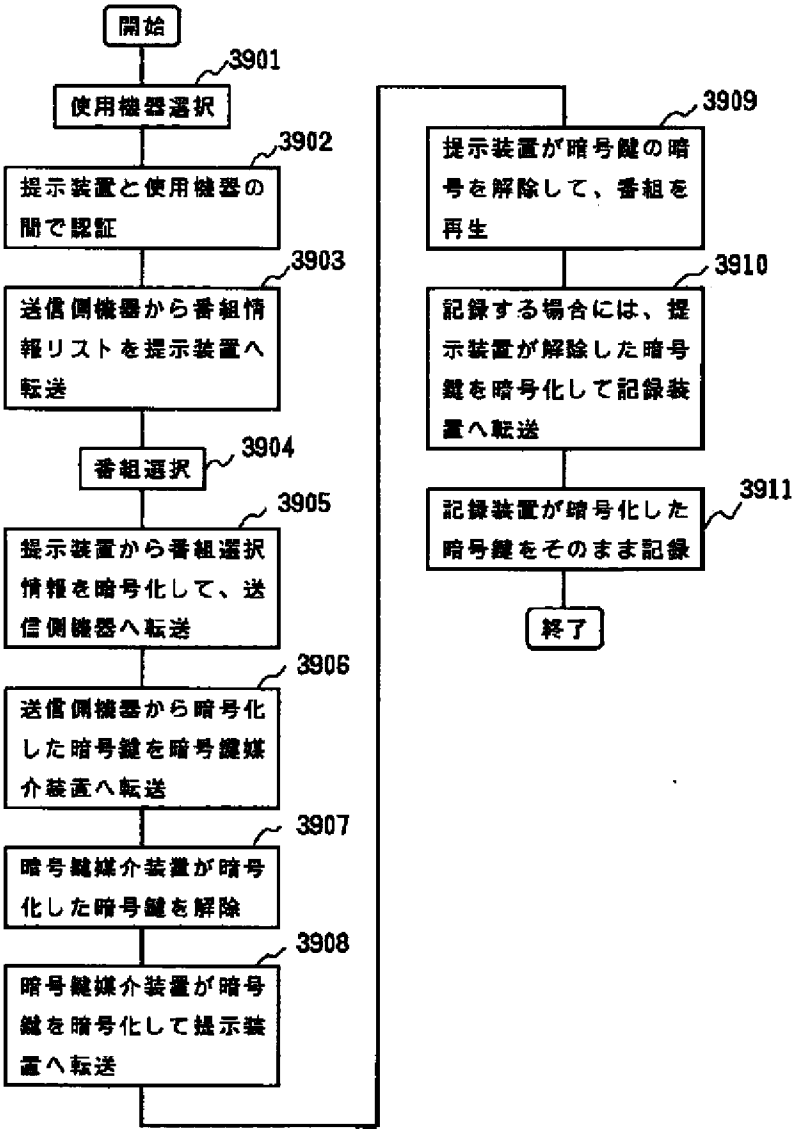
【図３８】

図 38


受信機
暗号鍵媒介装置
ＩＣカード
提示装置
3703
番組選択
認証処理
3702
認証処理
3704
暗号化した暗号鍵を転送
3705
3706
暗号解除
3707
暗号鍵を転送
3708
暗号鍵を暗号化
視聴開始時
認証処理
3709
認証通知
暗号化した暗号鍵を転送
3710
暗号化した暗号鍵を転送
3711
暗号化した番組を送信
3712
解除した暗号鍵で、番組の暗号を解除して再生

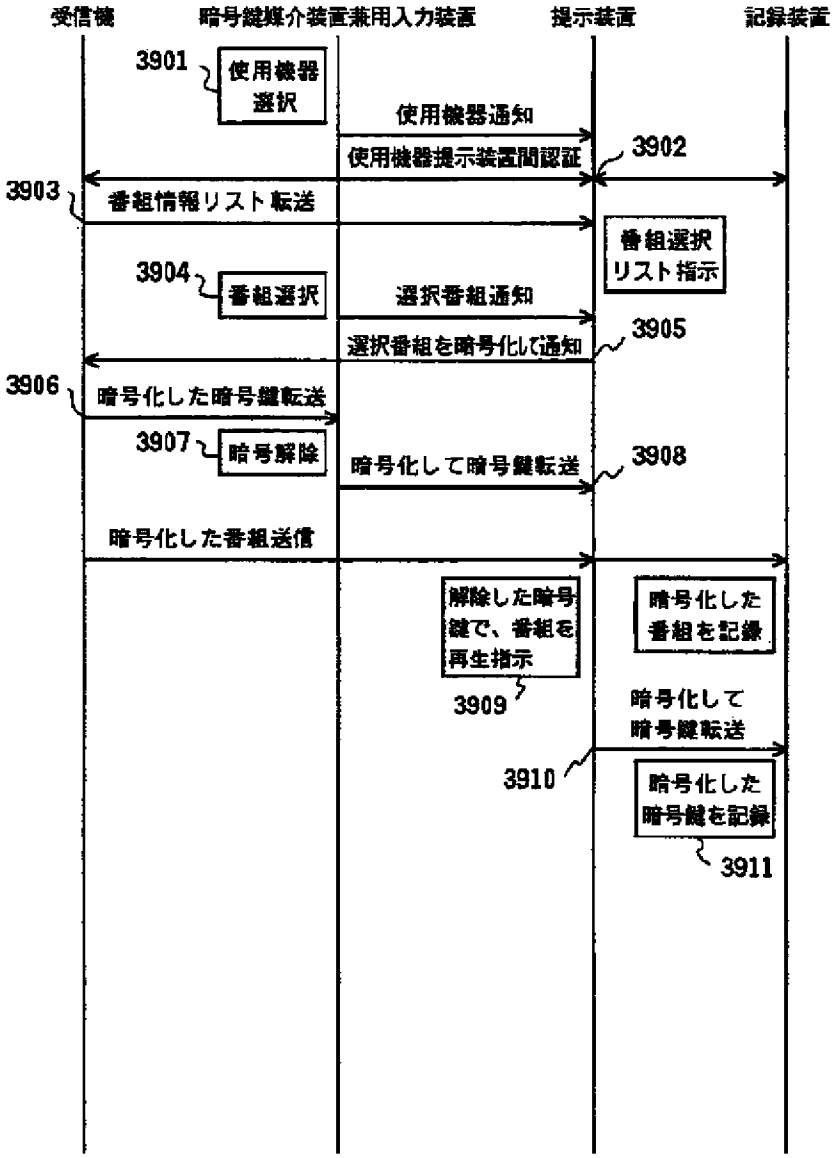
【図３９】

図 39


開始
3901
使用機器選択
3902
提示装置と使用機器の間で認証
3903
送信側機器から番組情報リストを提示装置へ転送
3904
番組選択
3905
提示装置から番組選択情報を暗号化して、送信側機器へ転送
3906
送信側機器から暗号化した暗号鍵を暗号鍵媒介装置へ転送
3907
暗号鍵媒介装置が暗号化した暗号鍵を解除
3908
暗号鍵媒介装置が暗号鍵を暗号化して提示装置へ転送
3909
提示装置が暗号鍵の暗号を解除して、番組を再生
3910
記録する場合には、提示装置が解除した暗号鍵を暗号化して記録装置へ転送
3911
記録装置が暗号化した暗号鍵をそのまま記録
終了

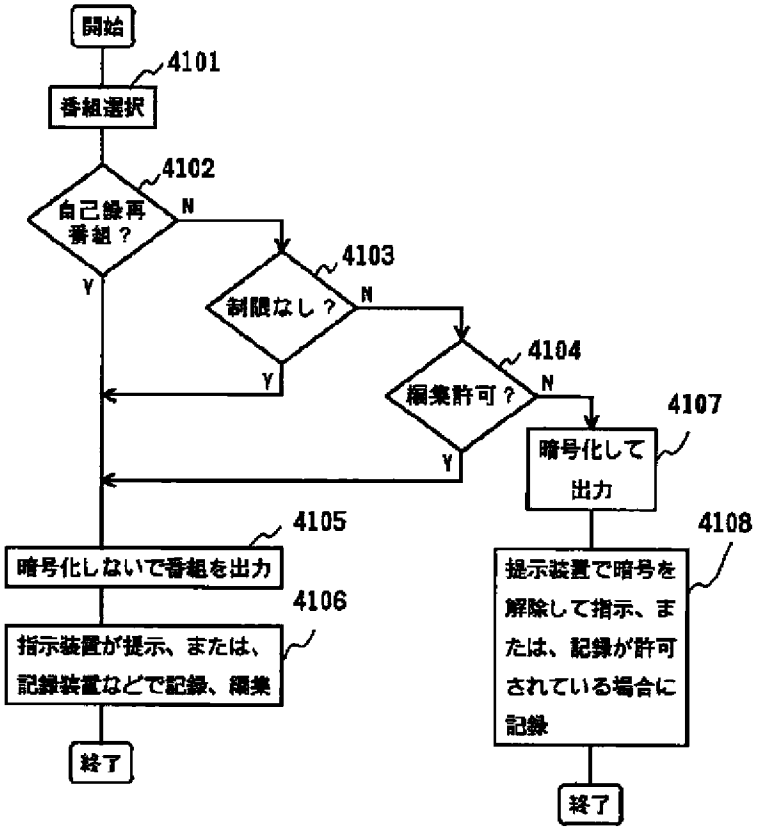
【図４０】

図 40


受信機
暗号鍵媒介装置兼用入力装置
提示装置
記録装置
3901
使用機器選択
使用機器通知
使用機器提示装置間認証
3902
3903
番組情報リスト転送
番組選択リスト指示
3904
番組選択
選択番組通知
選択番組を暗号化して通知
3905
3906
暗号化した暗号鍵転送
3907
暗号解除
暗号化して暗号鍵転送
3908
暗号化した番組送信
解除した暗号鍵で、番組を再生指示
3909
暗号化した番組を記録
暗号化して暗号鍵転送
3910
暗号化した暗号鍵を記録
3911

【図４１】

図　41



フロントページの続き

(51)Int.Cl.'	識別記号	FI	テーマコード(参考)
		H04N 7/167	Z

(72)発明者　高清水　聡
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　米田　茂
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　根本　敏之
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　鶴賀　貞雄
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　是枝　浩行
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　岡村　巧
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考) 5B017 AA03 BA07 BB09
5B035 AA13 BB09 BC03 CA38
5C053 FA13 FA21 FA25 GB37 JA30
5C064 CA14 CB01 CC04
5J104 AA13 AA15 AA16 EA06 EA19
NA02 NA35 NA37 PA05